



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



**Audit of Compliance with  
Standards Governing Combined  
DNA Index System Activities at  
the Los Angeles County Sheriff's  
Department Scientific Services  
Bureau Crime Laboratory  
Los Angeles, California**

**AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING  
COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE  
LOS ANGELES COUNTY SHERIFF'S DEPARTMENT  
SCIENTIFIC SERVICES BUREAU CRIME LABORATORY  
LOS ANGELES, CALIFORNIA**

**EXECUTIVE SUMMARY**

The Department of Justice Office of the Inspector General (OIG), Audit Division, has completed an audit of compliance with standards governing the Combined DNA Index System (CODIS) activities at the Los Angeles County Sheriff's Department (LASD) Scientific Service Bureau Crime Laboratory (LASD Laboratory) in Los Angeles, California.

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.<sup>1</sup> 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 January 2012 through January 2017. The objectives of our audit were to determine if: (1) the LASD Laboratory was in compliance with select NDIS Operational Procedures; (2) the LASD Laboratory was in compliance with certain Quality Assurance Standards (QAS)

---

<sup>1</sup> 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.

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

Our review determined the following:

- The LASD Laboratory did not limit and control access to its laboratory as required by NDIS's Security Requirements. Specifically, we found that there were former employees who had retained active keycards to restricted areas of the LASD Laboratory after their employment with the LASD had ceased. We also found keycards assigned to unknown individuals and individuals with inappropriate access to restricted areas of the LASD Laboratory. Further, we determined that the LASD Laboratory's distribution system for its keycards was not current, accurate, and clearly documented as required by the FBI's QAS. After we brought these security deficiencies to the attention of the LASD Laboratory Director, the LASD Laboratory deactivated the former employees' keycards and limited access to the restricted areas of the Laboratories as required.
- The LASD Laboratory did not provide adequate physical security for its CODIS server and client terminals against unauthorized personnel gaining access to the computer equipment or to the stored data. The LASD Laboratory was co-located with the Los Angeles Police Department Crime Laboratory on the fourth floor of a building shared with other organizations. We found more than 550 individuals had access to the fourth floor space where a client terminal was located, including former LASD employees (one of which also had access to the CODIS server room) and individuals whose employers we could not determine. We also determined that the LASD Laboratory did not have adequate security measures in place to protect against unauthorized personnel gaining access to DNA records or data. Specifically, we found CODIS specimen reports that were left next to a CODIS terminal located in a cubicle in the common area of the fourth floor.
- We reviewed 100 of the LASD Laboratory's 5,639 forensic profiles that were uploaded to NDIS as of January 2017. Of the 100 forensic profiles sampled, we ultimately found that 98 profiles were complete, accurate, and allowable. We identified one unallowable profile that was not attributable to the putative perpetrator, which the LASD Laboratory agreed and removed from CODIS. We also found one forensic profile that was uploaded to CODIS with an inaccurate allele, which the LASD Laboratory agreed and corrected. In addition, we found nine forensic profiles that were uploaded to CODIS prior to receiving a secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category, as required by the FBI. Finally, of the 100 forensic profiles that we selected, we initially found 16 forensic case files that lacked sufficient supporting documentation and information from which we could determine CODIS eligibility. After we informed the LASD Laboratory, it contacted the law enforcement agencies that had submitted the forensic profiles to obtain information on these 16 case files. Based on that information, we were able to test for CODIS eligibility and it resulted in the removal of one unallowable profile, described above.

We made eight recommendations to address the LASD Laboratory's compliance with standards governing CODIS activities, which are discussed in detail in the body of this report. Our audit objectives, scope, and methodology are detailed in Appendix 1 of the report and the audit criteria are detailed in Appendix 2. In addition, we requested written responses to our draft report from the LASD Laboratory and FBI. We received those responses and they are found in Appendices 3 and 4, respectively. Our analysis of those responses and the summary of actions necessary to close the report are found in Appendix 5.

**AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING  
COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE  
LOS ANGELES COUNTY SHERIFF'S DEPARTMENT  
SCIENTIFIC SERVICES BUREAU CRIME LABORATORY  
LOS ANGELES, CALIFORNIA**

**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
Inadequate Physical Security to the LASD Laboratory.....	6
Physical Access to the CODIS Server and Client Terminals .....	12
DNA Records and Data .....	13
Compliance with Certain Quality Assurance Standards .....	15
Internal and External QAS Reviews .....	15
Suitability of Forensic DNA Profiles in CODIS Databases .....	18
Lack of Documentation in its Case Files.....	19
Incorrect Profile.....	19
CODIS Eligibility Review Prior to NDIS Upload.....	20
Conclusion.....	20
Recommendations .....	21
APPENDIX 1: OBJECTIVES, SCOPE, AND METHODOLOGY.....	23
APPENDIX 2: AUDIT CRITERIA.....	25

APPENDIX 3: LABORATORY'S RESPONSE TO THE DRAFT AUDIT REPORT ..... 28

APPENDIX 4: THE FBI'S RESPONSE TO THE DRAFT AUDIT REPORT ..... 35

APPENDIX 5: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF  
ACTIONS NECESSARY TO CLOSE THE REPORT ..... 36

**AUDIT OF COMPLIANCE WITH STANDARDS  
GOVERNING COMBINED DNA INDEX SYSTEM ACTIVITIES  
AT THE LOS ANGELES COUNTY SHERIFF'S DEPARTMENT  
SCIENTIFIC SERVICES BUREAU CRIME LABORATORY  
LOS ANGELES, CALIFORNIA**

The Department of Justice Office of the Inspector General (OIG), Audit Division, has completed an audit of compliance with standards governing the Combined DNA Index System (CODIS) activities at the Los Angeles County Sheriff's Department (LASD) Scientific Services Bureau Crime Laboratory (LASD Laboratory) in Los Angeles, California.

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.<sup>1</sup> 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 covered the period from January 2012 through January 2017. The objectives of our audit were to determine if: (1) the LASD Laboratory was in compliance with select National DNA Index System (NDIS) Operational Procedures; (2) the LASD Laboratory was in compliance with certain Quality Assurance Standards (QAS) issued by the FBI; and (3) the LASD 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, whereas Appendix 2 contains the criteria used to conduct the audit. We discussed the results of our audit with the LASD Laboratory and FBI officials and have included their comments in the report, as applicable. In addition, we received written responses from the LASD Laboratory and FBI, which can be found in Appendices 3 and 4, respectively. Our analysis of those responses and the summary of actions necessary to close the report are found in Appendix 5.

**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

---

<sup>1</sup> 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.

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.<sup>2</sup>

### *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**

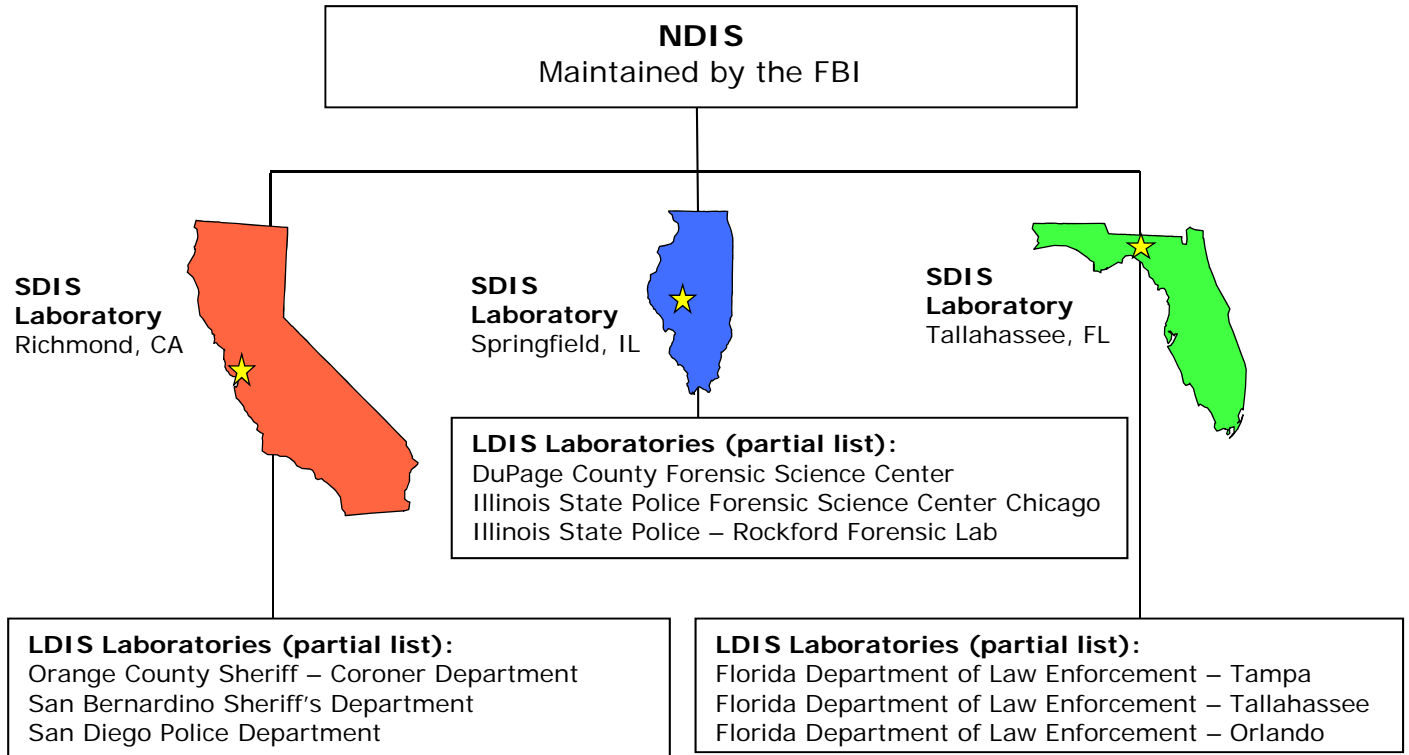
The FBI implemented CODIS as a distributed database with hierarchical levels that enables federal, state, and local crime laboratories to compare DNA profiles electronically. CODIS consists of a hierarchy of three distinct levels: (1) NDIS, managed by the FBI as the nation's DNA database containing DNA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

---

<sup>2</sup> 42 U.S.C.A. § 14132 (2006).



### 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 12 searchable indices:

- Convicted Offender Index contains profiles generated from persons convicted of qualifying offenses.<sup>3</sup>
- 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.

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

- 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 and/or that may indicate a possibility of allelic dropout.
- Missing Person Index contains known DNA profiles of missing persons and deduced missing persons.
- Unidentified Human (Remains) Index holds profiles from unidentified living individuals and the remains of unidentified deceased individuals.<sup>4</sup>
- 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 these 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 vetted against the Forensic, Convicted Offender, Arrestee, Detainee, and Legal Indices to provide investigators with leads in solving missing and unidentified person cases.

---

<sup>4</sup> 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.<sup>5</sup> 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 LASD Laboratory that we audited is co-located with the Los Angeles Police Department Crime Laboratory on the fourth floor of the Hertzberg-Davis Forensic Science Center (which also houses the California State University, Los Angeles School of Criminal Justice and Criminalistics, and California Forensic Institute) located in Los Angeles, California. The LASD Laboratory serves approximately 83 law enforcement agencies, including 30 Los Angeles County Sheriff's Department stations, the California State University Police Department, the U.S. Secret Service, and other law enforcement agencies. In total, the Laboratory serves a population size of more than 10 million people. The Laboratory participates in the CODIS program as a 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 1994. In July 2015, the

---

<sup>5</sup> 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.

Laboratory was accredited for 4 years by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB). Thus, the LASD Laboratory's accreditation will be up for renewal in July 2019.

### **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 LASD Laboratory did not fully comply with the NDIS Security Requirements that require an NDIS participating laboratory to have controlled access to its laboratory and laboratory assets. Specifically, we found that the LASD Laboratory had former employees still in possession of active keycards, keycards assigned to unknown individuals, and individuals with inappropriate access to areas of the LASD Laboratory. We also found that the LASD Laboratory did not provide adequate physical security for its CODIS server and client terminals, which increased the risk of unauthorized personnel gaining access to the computer equipment and any of the information stored within the equipment. Lastly, we found that the LASD 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 LASD Laboratory*

The FBI is responsible for ensuring the appropriate physical security for NDIS, while the NDIS participating laboratory must provide adequate physical security for the CODIS servers and clients. As previously stated, the LASD Laboratory is located on California State University's campus in a building that is shared by the University, the LASD Laboratory, and the Los Angeles Police Department (LAPD) Laboratory. The building is accessible to the public during regular business hours but requires a keycard for entry after-hours and on the weekends. The LASD and LAPD Laboratories share one floor.<sup>6</sup> The main public entrance to the building is located on the second floor but authorized personnel can gain further entry to the vestibule, which leads to a bank of elevators, with a keycard.<sup>7</sup> Once inside the elevators, authorized personnel must swipe their keycard that is specifically coded for the fourth floor, where the LASD Laboratory is located, in order to gain access. During our visit and tour, we asked the CODIS Administrator how many staff members had physical access to the fourth floor and

---

<sup>6</sup> The LASD Laboratory shares its CODIS server room, pre-amplification room, and post-amplification room with the LAPD Laboratory.

<sup>7</sup> Authorized personnel may also use their keycards to access the first floor south entrance. Elevators provide access to all secure areas of the building, including the first floor.

we were provided a keycard distribution list of 877 active keycards, which provide access to the fourth floor.<sup>8</sup>

Former Employees 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, all exterior entrance and exit points require security control and the distribution of all keys and combinations shall be documented and limited to the personnel designated by laboratory management. Moreover, the LASD Laboratory’s policy requires that the assignment of keycards issued to employees be documented on its keycard request form and when staff no longer work at the LASD Laboratory, the return of all keycards are to be documented on the same form. Each keycard is assigned multiple access permissions to different areas of the LASD Laboratory. We found that the LASD Laboratory failed to properly collect and deactivate keycards when employees departed the LASD Laboratory. Based on our review of the keycard distribution list, we determined that eight former LASD employees had active keycard access to the second floor vestibule and to the fourth floor at the time of our audit. As shown in Table 1, we also determined that the eight former employees had access to restricted areas of the Laboratories.

**Table 1**  
**Former LASD Employees’ Areas of Access**

Number of Former Employees	Areas of Access
1	CODIS room
2	DNA freezer room
2	Pre- and post-amplification rooms
5	Crime scene room
7	Exam room
7	Extraction room

Source: LASD Laboratory and OIG

We asked the LASD Laboratory Director, Assistant Director, and the CODIS Administrator whether or not the keycards had been collected before each employee’s departure. In response, the CODIS Administrator provided us the keycard request forms for each of the eight former employees, which indicated that the keycards had not been returned to the LASD Laboratory upon their departure. Nearly a month after our initial site visit and after asking LASD Laboratory officials to review its keycard distribution list for former employees who still held active keycards, a LASD Laboratory official provided us evidence that all eight former

---

<sup>8</sup> The 877 active keycards represent 309 LASD personnel, 424 LAPD personnel, and 144 other keycards, the assignment to whom could not be determined.

employees' keycards were deactivated on March 8, 2017, 23 days after we began our audit.

**Table 2**  
**Former LASD Employees with Active Keycards**

Former Employee Count	Date of Separation	Date the Keycard was Deactivated	Length of Time to Deactivate Keycards (months)
1	11/02/14	03/08/17	29
2	10/13/15	03/08/17	17
3	11/30/15	03/08/17	15
4	03/31/16	03/08/17	11
5	03/31/16	03/08/17	11
6	05/31/16	03/08/17	9
7	08/31/16	03/08/17	6
8	11/30/16	03/08/17	3

Source: LASD Laboratory and OIG

As reflected in Table 2, five of the former employees held active keycards for 11 months or more after ceasing employment with the LASD Laboratory; the most egregious example was a keycard that remained active approximately 2.5 years after the employee's departure. To issue new keycards, the keycard request form must have the approval and signature of the LASD Laboratory's Assistant Director, the unique keycard number, the date it was assigned, and to whom it was assigned. However, the form did not contain a specific section to document the collection date of returned keycards and who took possession of the returned keycards. This practice increases the risk that both information and evidence may be inappropriately accessed or mishandled and compromises the security of the Laboratory, as well as the privacy right of individuals whose information is maintained by the Laboratory. Therefore, we recommend that the FBI work with the LASD 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' keycards have been deactivated.

Individuals with Inappropriate Access to Areas of the Laboratory

As previously mentioned, NDIS participating laboratories are required to have limited and controlled access to the laboratory and laboratory assets. According to the LASD Laboratory's policy, access to the facility and areas within the facility is authorized by the Laboratory Director through an appropriate designee, such as the Assistant Laboratory Director or the Facility Manager. We judgmentally selected a sample of 88 of the 301 keycards (29 percent) listed on the LASD Laboratory's keycard distribution list to determine whether the individuals

associated with the keycards were eligible for the corresponding access to the fourth floor and areas of the LASD Laboratory.<sup>9</sup>

Based on our review, we determined that 57 keycards, issued to 45 individuals, provided access to areas of the LASD Laboratory that were not required in order to perform their job responsibilities. For instance, we found that a plumber had access to the evidence exam room, where, based on LASD Laboratory policy, evidence is allowed to be left out until the end of the work day, at which time the evidence is required to be secured. In addition, we found that an IT Specialist had access to the DNA freezer room, where the freezers containing DNA evidence are not individually locked within the room. The CODIS Administrator agreed that the 45 individuals had inappropriate access to either the fourth floor or to certain areas of the Laboratory, but he did not provide an explanation as to how or why this occurred. We received an updated keycard distribution listing, showing that the LASD Laboratory restricted the access rights for 43 individuals and the 54 keycards that were assigned to them. The LASD Laboratory still needs to remedy the remaining individuals' inappropriate access rights.

---

<sup>9</sup> The 301 keycards were assigned to LASD personnel, contractors, and volunteers that work at the LASD Laboratory. We did not include keycards issued to the LASD Laboratory's former employees. In addition, we did not review LAPD Laboratory employees' access to the fourth floor and laboratory spaces.

**Table 3**  
**Restrictions on Individuals' Keycard Access**

<b>Position Title<sup>a</sup></b>	<b>Count of LASD Individuals</b>	<b>Areas of Access Removed<sup>b</sup></b>	<b>Number of Access Rights Removed<sup>c</sup></b>
Assistant Director	1	CODIS room	1
Electrician Supervisor	1	Main entrance	1
General Maintenance Worker	3	Main entrance	3
Information Systems Analyst II	1	Crime scene room, Extraction room, Freezer room, Pre- and Post-amplification rooms	5
Intermediate Clerk	1	Exam room, Extraction room	2
Intermediate Typist Clerk	4	Exam room, Extraction room	8
IT Specialist	1	Extraction room, Freezer rooms, Pre- and Post-amplification rooms	4
Office Assistant II	1	Exam room, Extraction room	2
Operations Assistant I	3	Exam room, Extraction room	6
Operations Assistant II	2	Exam room, Extraction room	4
Operations Assistant III	2	Exam room, Extraction room	4
Painter	3	Main entrance	3
Photographer I	3	Extraction room	3
Photographer II	5	Extraction room	5
Plumber <sup>d</sup>	2	Main entrance, Extraction room, Exam room, Pre- and Post-amplification rooms	6
Refrigeration Mechanic	1	Main entrance	1
Secretary	1	Exam room, Extraction room	2
Senior Criminalist	1	CODIS room	1
Senior Typist Clerk	2	Exam room, Extraction room	4
Steam Fitter	1	Main entrance	1
Supervising Criminalist	3	CODIS room	3
Supervising Photographer	1	Extraction room	1
Volunteer - Chaplain	1	Main entrance	1
Volunteer Forensic Document Examiner	1	Extraction room	1
	<b>45</b>		<b>72</b>

<sup>a</sup> The position title can represent more than one employee.

<sup>b</sup> Access rights to the main entrance includes elevator access to each of the facility's floors.

<sup>c</sup> Each keycard is assigned multiple access permissions to different areas of the LASD Laboratory.

<sup>d</sup> Each of the plumbers had their main entrance access rights removed. One of the plumbers also had access rights to the Extraction room, Exam room, and Pre- and Post-amplification rooms, which the LASD Laboratory has removed.

Source: LASD Laboratory and OIG



Allowing individuals unrestricted access to areas of the Laboratories that are unnecessary for the performance of their job responsibilities is a violation of NDIS Security Requirements and poses a risk to DNA evidence, case work analysis, laboratory equipment, and other law enforcement sensitive information. Therefore, we recommend that the FBI work with the LASD Laboratory to ensure that all individuals (including LASD personnel, contractors, and volunteers) have appropriate access to the fourth floor, areas within the LASD Laboratory, and to the LASD Laboratory's assets.

#### Unassigned and Duplicate Keycards

According to NDIS Security Requirements, the distribution of all keycards are required to be documented and limited to personnel designated by laboratory management. As shown in Table 4, the CODIS Administrator provided us a keycard distribution list of 877 active keycards that have access to the fourth floor where the LASD Laboratory is located.

**Table 4**  
**Physical Access to the 4<sup>th</sup> Floor**

Physical Access	Number of Active Keycards
LAPD Employees	424
LASD Employees	309
Visitors	77
Unknown <sup>a</sup>	49
Loaners <sup>b</sup>	11
Emergency Employees	7
<b>Total</b>	<b>877</b>

<sup>a</sup> Keycards with no name assigned, an incomplete name listed, or the agency for whom the employee worked was unable to be determined.

<sup>b</sup> Keycards assigned to employees who forgot their keycards.

Source: LASD Laboratory and OIG

We were unable to determine to whom 49 of the keycards were issued: (a) 5 keycards had no name associated with the keycard; (b) 1 keycard had an incomplete name, where the last name was missing; and (c) the employer for whom the individual worked was undeterminable for 43 keycards. We asked the CODIS Administrator why the distribution list contained so many inaccuracies. The CODIS Administrator did not state why the distribution list was inaccurate, but did agree that the keycard distribution list needed to be reviewed and updated. Based on the LASD Laboratory's policy, a verification of issued keycards is required during the annual quality assurance review. During the LASD Laboratory's last internal review conducted in May 2016 there were no findings with regard to the

Laboratory's physical security and distribution of keycards. We discuss this matter further in the Internal and External QAS Reviews section below.

We also determined that 214 of the 877 active keycards (24 percent) were assigned to individuals in duplicate. Each of the keycards issued had a unique identifying serial number. Out of the 214 keycards issued to individuals in duplicate, 28 were assigned to 24 LASD Laboratory employees.<sup>10</sup> Of those 24 LASD personnel, we found that: (1) 21 had duplicate access to the evidence exam and extraction rooms; (2) 14 had duplicate access to the crime scene room; (3) 8 had duplicate access to the pre- and post-amplification rooms; (4) 7 had duplicate access to the DNA freezer rooms; and (5) 6 had duplicate access to the CODIS server room. We asked the LASD Laboratory Director why multiple keycards had been provided to personnel and he stated that it was necessary to assign more than one keycard to some individuals to keep in a different location, like he does by keeping a keycard in his vehicle in case he forgets the keycard that he usually carries with him. The Director also stated that not all employees have returned their original keycards after being provided additional keycards when the facility's keycard access system had undergone a change. As of July 2017, 19 of the 24 LASD personnel still had active duplicate keycards, which we believe should be returned to the LASD Laboratory and deactivated.

Providing keycards to individuals without properly documenting to whom the keycards were assigned and assigning cards in duplicate to employees increases the risk of loss and theft of a keycard while at the same time weakening controls that could prevent unauthorized access to the Laboratory, including restricted areas within the Laboratory. Therefore, we recommend that the FBI work with the LASD Laboratory to ensure that the distribution of all keycards are properly documented and limited to personnel designated by Laboratory management, including performing a review of all unknown keycards and deactivating duplicate keycards.

#### *Physical Access to the CODIS Server and Client Terminals*

The NDIS Security Requirements state that participating laboratories are required to provide adequate physical security for the CODIS server and client terminals against any unauthorized personnel gaining access to the computer equipment or to any of the stored data. Placing a CODIS server or a client terminal 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. We determined that the CODIS server and four client terminals were stored in the server room, which requires keycard to access and the CODIS Administrator stated that access to the CODIS server room was limited to CODIS users.<sup>11</sup> However, we determined that one former employee that no longer works at the LASD Laboratory had keycard access for approximately 2.5 years after their employment with the LASD Laboratory had ended. The CODIS Administrator provided documentation

---

<sup>10</sup> The remaining 186 keycards were assigned to LAPD Laboratory employees.

<sup>11</sup> The LASD Laboratory shares its CODIS server room with the LAPD Laboratory.

that confirmed the employee's keycard had never been returned prior to the employee leaving. In addition, five LASD Laboratory employees that were former CODIS users still had keycard access to the CODIS server room at the time of our audit.<sup>12</sup> Unauthorized personnel, such as former employees, should not have keycard access to the CODIS server and client terminals located in the CODIS server room. After we informed the LASD Laboratory, the CODIS Administrator provided us evidence that both the former employee's keycard had been deactivated and that the 5 former CODIS users' keycards had been restricted.

The LASD Laboratory also maintains one client terminal in the CODIS Administrator's office, which is locked and secure when the CODIS Administrator is not there, and one other client terminal that is located in a cubicle in the common area on the fourth floor. The CODIS Administrator stated that the CODIS client terminal located in the cubicle space was not a security risk because access to the fourth floor was limited and controlled. We disagree with the CODIS Administrator's statement because, as previously discussed, we believe that access to the LASD Laboratory was not limited and controlled as required by NDIS's Security Requirements. The fact that the keycard access system is shared with another agency (LAPD Laboratory) indicates that the LASD Laboratory does not have exclusive control over who has access to its space on the fourth floor. Further, as mentioned before, we found weaknesses with the LASD Laboratory's controls over keycards that were improperly assigned to former LASD Laboratory employees, unknown individuals, and unauthorized individuals allowing such individuals access to the fourth floor of the LASD Laboratory. Based on the issues we have identified, we believe that there is serious risk of unauthorized access to the LASD Laboratory and the client terminal located in the common area of the fourth floor. Therefore, we recommend that the FBI ensure that the LASD Laboratory strengthen physical security over the CODIS server and client terminals to prevent any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

### *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 nor authorized to access such DNA records under the Act. During our site visit, we observed that the LASD Laboratory's DNA analysts sit in cubicles in a common area on the fourth floor, which was accessible by the more than 550 individuals. We found CODIS specimen reports left on a desk sitting next to the CODIS client terminal in a cubicle in the common area. When we asked why the specimen reports were left there, the CODIS Administrator stated that CODIS users would leave the specimen reports

---

<sup>12</sup> We also found two former personnel from the LAPD that no longer work at the LAPD Laboratory who also had active keycards to the CODIS server room.

next to the CODIS client terminal for the Technical and Administrator reviewers' reference when reviewing the DNA case file prior to its upload into CODIS. Based on the security risks we have previously identified, including unauthorized access to the fourth floor, the LASD Laboratory is at an increased risk that both information and evidence may be inappropriately accessed or mishandled, which compromises the security of the Laboratory, as well as the privacy rights of individuals whose information is maintained by the Laboratory. Therefore, we recommend that the FBI work with the LASD Laboratory to ensure that it has adequate physical security measures in place to protect against unauthorized personnel gaining access to any DNA records or data.

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

- 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 4 of the LASD Laboratory's 40 CODIS users and asked if they were aware of the NDIS procedures and knew how to access them. All four 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 40 CODIS users and 1 Information Technology CODIS user.
- CODIS users are required to annually complete DNA Records Acceptance training. The FBI provided us a list of LASD Laboratory personnel who had completed this mandatory annual training. We determined that each of the Laboratory's 40 CODIS users had successfully completed the FBI's annual training for 2016 and 2017.
- The FBI provides guidance for participating laboratories to follow when confirming matches that are identified in the CODIS system. We reviewed a judgmentally selected sample of 10 NDIS matches and determined that:
  - The LASD Laboratory sent confirmation requests in a timely manner for all 10 matches;
  - Confirmation generally took place within 30 days after the originating laboratory's request was sent out; and
  - The LASD Laboratory notified investigators of match confirmation within 5 days for all 10 matches.
- The NDIS participating laboratory is required to adhere to specific NDIS Security Requirements related to the backup and storage of its CODIS data. We determined that the LASD Laboratory adhered to these requirements.

- There are specific security requirements that an NDIS participating laboratory is required to follow in order to ensure the security of CODIS software, user accounts, servers, and terminals. We judgmentally selected 4 of the LASD Laboratory's 40 CODIS users and verified that each of the 4 CODIS users were adhering to the NDIS Security Requirements. We did identify one additional CODIS user account that was no longer being used but was still active in CODIS. The CODIS Administrator stated that the user's ability to sign in had been disabled years ago, but he agreed to also deactivate the account in CODIS. The FBI confirmed that the account was not in NDIS and had no capabilities to add or alter any information in NDIS. Based on this evidence and the LASD Laboratory's corrective actions, we make no recommendation on this finding.

### **Compliance with Certain Quality Assurance Standards**

During our audit, we considered the Forensic QAS issued by the FBI.<sup>13</sup> These standards describe the quality assurance requirements that the LASD Laboratory must follow to ensure the quality and integrity of the data it produces. We also assessed the two most recent QAS reviews that the LASD Laboratory underwent.<sup>14</sup> The QAS we reviewed are listed in Appendix 2 of this report.

We found that security at the LASD Laboratory did not meet the FBI's QAS standards that outline controlled access to the LASD Laboratory. Specifically, we found that the LASD Laboratory's distribution list of keycards was inaccurate and not up to date as required by the FBI. 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 review document, asks if the distribution of all keys and combinations are documented and limited to personnel designated by laboratory management. We found that on both the LASD Laboratory's 2015 external review and 2016 internal review that the reviewer 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 ensuring that the distribution system of all keys and combinations are current, accurate, clearly documented, and available for

---

<sup>13</sup> Forensic Quality Assurance Standards refer to the Quality Assurance Standards for Forensic DNA Testing Laboratories, effective September 1, 2011.

<sup>14</sup> 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 auditors, from an external agency. These audits are not required by the QAS to be performed in accordance with generally accepted government auditing standards and are not performed by the Department of Justice Office of the Inspector General. Therefore, in this report 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 generally accepted government auditing standards.

review. We believe that the LASD Laboratory's keycard distribution list was outdated and inaccurate as former personnel had active keycards (one former employee since November 2014), unknown individuals had been assigned keycards, and individuals had inappropriate keycard access to areas of the Laboratories. The LASD Laboratory's policy also required that issued keycards be verified during the annual QAS review. We asked the CODIS Administrator if the LASD Laboratory annually reviewed the distribution list and verified the keycards that were issued. The CODIS Administrator stated that the QAS reviewer typically selects a sample of keycards to review and verify. Based on the security risks we have identified during our audit and the fact that both the internal and external QAS reviews failed to detect the LASD Laboratory's security issues, we believe that the LASD Laboratory should ensure that it does a better job of performing its internal QAS review, paying special attention to the LASD Laboratory's adherence to QAS Standard 6. Further, to rectify the security deficiencies we identified, the LASD Laboratory should review the entire keycard distribution list rather than just a sample of keycards and ensure that all keycard holders that have been granted access rights still require those access rights. Therefore, we recommend that the FBI work with the LASD Laboratory to ensure that it adequately performs its internal QAS reviews to verify compliance with each QAS, including ensuring that the distribution of all keycards are current, accurate, clearly documented, and available for review.

We found that the LASD 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 2015 and 2016, we determined that the Laboratory had an external QAS review performed in March 2015 and an internal QAS review performed in May 2016, in accordance with the FBI's requirement.
- We reviewed the LASD 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 March 2015, noted no findings for the LASD Laboratory.
  - The internal QAS review conducted in May 2016, noted no findings for the LASD 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 LASD Laboratory's March 2015 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 LASD Laboratory had separate areas for DNA examination and extraction, PCR setup, and DNA amplification. The LASD Laboratory was physically separated into pre-PCR and post-PCR areas and during our site visits we observed 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 LASD Laboratory. We also observed designated laboratory coats (distinguished by color) were used in the pre- and post-amplification rooms to prevent contamination.
- The Laboratory's policy for controlling and safeguarding evidence samples requires that all evidence be kept in the evidence vault or in an alternative evidence storage location within the LASD Laboratory and that the Laboratory must be locked and secured during off-duty hours. We observed that the LASD Laboratory's vault was secure and access to it was limited to authorized laboratory personnel only. The chain of custody over evidence was documented in the Laboratory's evidence retrieval system, known as the Property and Evidence Information Management System (PRELIMS). According to the LASD Laboratory's policy, PRELIMS maintains information on the location of each piece of evidence at all times. When a DNA analyst makes a request to sign out evidence from the vault, the sign-out process includes the DNA analyst scanning a unique bar code on the evidence's identification tag to document the chain of custody in PRELIMS. DNA analysts are assigned locked refrigerators or storage spaces to secure the evidence while it is not in the DNA analyst's immediate custody. Upon completion of DNA analysis, the DNA Analyst returns the evidence to the vault, where it is scanned back in by the property and evidence custodian. Due to limited storage space at the LASD Laboratory, all evidence is preserved by the LASD Laboratory while DNA analysis is being conducted and returned to the submitting agency once the analysis is complete. Based on our observations, the LASD Laboratory maintained integrity of its physical evidence in accordance with the QAS requirements that we tested.
- The FBI's QAS requires NDIS participating laboratories to ensure that its vendor laboratories undergo an external review once every 2 years and an internal review every year, and maintain their accreditation. In addition, NDIS participating laboratories are required to perform annual site visits to its vendor laboratories.<sup>15</sup> Between February 2015 and February 2017, the LASD Laboratory outsourced the review of its forensic profiles to four vendor laboratories. As of February 2017, each of the four vendors were

---

<sup>15</sup> The FBI's QAS requires that NDIS participating laboratories perform an initial on-site visit to its vendor laboratories prior to a vendor performing casework analysis for the laboratory. For contracts lasting longer than a year, annual on-site visits are also required. The FBI will accept an on-site visit conducted by the NDIS participating laboratory, a designated FBI employee, or another NDIS participating laboratory using the same technology, platform, and typing test kit.

accredited, had undergone the required external and internal QAS reviews, and resolved the noted reviews' findings. We also determined that either the LASD Laboratory or another NDIS participating laboratory performed annual site visits to each of the four vendors, as required by the FBI.

- The FBI's QAS requires a CODIS Administrator or technical reviewer to review outsourced DNA data and to verify specimen eligibility and the correct specimen category for entry into CODIS. We judgmentally selected 6 of 30 outsourced forensic DNA profiles and determined that the LASD Laboratory had technically reviewed the DNA data prior to upload and verified the specimen's eligibility for CODIS.

### **Suitability of Forensic DNA Profiles in CODIS Databases**

We reviewed a sample of the LASD 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 to include each value returned at each locus for which the Laboratory 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 sample of 100 profiles out of the 5,639 forensic profiles the LASD Laboratory had uploaded to NDIS as of January 2017. Of the 100 forensic profiles sampled, we found 1 unallowable profile that was not attributable to the putative perpetrator and 1 incorrect profile that was uploaded to CODIS with an inaccurate allele. The specific exceptions are explained in more detail below. In addition, we determined that 16 of the 100 case files we reviewed did not contain enough information to determine CODIS eligibility and 9 forensic profiles that were uploaded to CODIS prior to receiving a secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category, as required by the FBI.



### *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 or not a DNA profile is eligible for NDIS, a DNA analyst must have enough information to determine if a crime was committed, what type of crime had occurred, and if the evidence was attributable to a putative perpetrator. In May 2014, the FBI conducted a NDIS participation assessment and as a result, it was determined that the LASD Laboratory did not consistently document or verify CODIS eligibility information for its forensic profiles uploaded to CODIS. The LASD Laboratory took corrective action by informing all DNA Analysts that supporting documentation was required when determining CODIS eligibility. A DNA analyst stated that she relied on the crime scene report form from the investigator, which requires that the investigator circle either "yes" or "not sure" as to whether the evidence collected at the crime scene is attributable to a putative perpetrator, in order to determine CODIS eligibility. We found that 16 of the 100 sampled case files did not contain sufficient information in order for us to determine whether or not a forensic profile was eligible for CODIS. The CODIS Administrator contacted the law enforcement agency (LEA) for each of the 16 forensic profiles in question in order to obtain additional information. Based on the LEA's information, we determined that 15 of the profiles were eligible for upload into NDIS and that 1 profile, Sample Item 27, was determined not to be eligible and was removed from CODIS. We recommend that the FBI work with the LASD Laboratory to ensure that all case files contain sufficient information in order to determine CODIS eligibility.

#### Sample Item 27

Sample Item 27 was a cigarette butt found on the floor of a crime scene. We determined that the case file contained no information about the crime or crime scene where the cigarette butt was taken from. We asked the CODIS Administrator about the DNA profile and if a crime had occurred. The CODIS Administrator stated that the DNA analyst relied on a form which is completed by the investigating officer stating that the evidence was attributable to a putative perpetrator. According to the NDIS Operational Procedures, a forensic unknown, forensic mixture, or forensic partial DNA record submitted to NDIS shall originate from and/or be associated with a crime scene; the source of which is attributable to a putative perpetrator. Relying on a form without knowing what crime had occurred or where the DNA profile was taken from does not fulfill the NDIS requirements. The CODIS Administrator contacted the LEA who had collected the DNA profile and the LEA stated that the evidence should not have been analyzed for DNA and that the DNA specimen should be removed from CODIS. The CODIS Administrator agreed with the LEA, removed the unallowable profile from CODIS, and provided us the specimen delete report while we were on-site.

#### *Incorrect Profile*

According to the FBI's NDIS Operational Procedures, database and reference samples shall be accurate and complete for the CODIS Core Loci. In addition, if a

DNA record is submitted to NDIS and then found to be inaccurate, it shall either be modified to achieve accuracy or deleted from NDIS by the submitting agency. During our audit, we identified a profile that had been uploaded to NDIS with an incorrect allele.

### Sample Item 38

Sample Item 38 was obtained from a sexual assault kit. Reference samples were also collected from the victim and suspect. We deemed this profile to be inaccurate as an allele call on the specimen detail report did not match the allele call on the electropherogram report within the case file. Upon reviewing the case file, the CODIS Administrator agreed with our assessment, corrected the error, and provided us the revised specimen detail report reflecting the change while we were on-site.

### *CODIS Eligibility Review Prior to NDIS Upload*

According to the FBI's QAS for Forensic DNA Testing Laboratories, all cases are required to be technically reviewed by a qualified DNA analyst for clerical and technical accuracy and the completion of the technical review must be documented. In addition, prior to uploading or searching a DNA profile in CODIS, the technical reviewer must verify the following criteria: (1) the DNA profile is eligible for CODIS upload; (2) the correct DNA type has been entered; and (3) the appropriate specimen category has been selected. Prior to entry of a DNA profile into a searchable category at SDIS, a concordant assessment (secondary review) for CODIS eligibility, correct DNA types, and the appropriate specimen category by a qualified analyst or technical reviewer is required by the FBI's QAS.

The LASD Laboratory documents its CODIS eligibility review on a paper form called the CODIS data verification form, which documents the initial and secondary review for CODIS eligibility. We determined that the LASD Laboratory uploaded to CODIS nine forensic profiles prior to receiving a secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category. We also found one forensic profile missing the signature attesting to the completion of a secondary review and another forensic profile that was missing the date of its secondary review; therefore, we could not determine if both underwent a secondary review prior to being entered into CODIS. The CODIS Administrator stated that he did not know why the verification forms were incomplete or completed after the forensic profiles had been uploaded. Therefore, we recommend that the FBI work with the LASD Laboratory to ensure that all DNA profiles, prior to being uploaded into CODIS, receive a concordant assessment for CODIS eligibility, correct DNA types, and the appropriate specimen category.

### **Conclusion**

We identified a number of issues with the LASD Laboratory's security and implementation of NDIS Procedures. Specifically, we found that the LASD Laboratory did not limit and control access to its laboratory as required by NDIS's

Security Requirements and that its system for distributing keys and combinations was not current, accurate, and clearly documented as required by the FBI's QAS. We also found that the LASD Laboratory failed to provide adequate physical security for its CODIS server, client terminals, and DNA records against any unauthorized personnel gaining access to the computer equipment or to any of the LASD Laboratory's stored data or DNA records.

Moreover, based on our testing of 100 LASD Laboratory forensic profiles that had been uploaded to NDIS, we determined that 1 DNA profile was inaccurate, 1 DNA profile was ineligible, and 16 case files lacked sufficient information to determine NDIS eligibility. The LASD Laboratory agreed and took corrective actions to resolve these matters while we were on-site. However, we also found that the Laboratory had uploaded to CODIS nine forensic profiles prior to receiving a secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category, as required by FBI.

## **Recommendations**

We recommend that the FBI:

1. Ensure that the LASD Laboratory implements the required physical access controls to properly track and maintain its distribution of keycards to ensure that all former employee's keycards have been deactivated.
2. Ensure that all individuals (including LASD personnel, contractors, and volunteers) have appropriate access to the fourth floor, areas within the LASD Laboratory, and to the LASD Laboratory's assets.
3. Ensure that the distribution of all keycards are properly documented and limited to personnel designated by laboratory management, including performing a review of all unknown keycards and deactivating duplicate keycards.
4. Ensure that the LASD Laboratory strengthen physical security over the CODIS server and client terminals against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.
5. Ensure that the LASD Laboratory has adequate physical security measures in place to protect against unauthorized personnel gaining access to any DNA records or data.
6. Ensure that the LASD Laboratory adequately performs its internal QAS reviews to verify compliance with each QAS, including ensuring that the distribution of all keycards are current, accurate, clearly documented, and available for review.
7. Ensure that all case files contain sufficient information in order to determine CODIS eligibility.

8. Ensure that all DNA profiles prior to being uploaded into CODIS receive a concordant assessment for CODIS eligibility, correct DNA types, and the appropriate specimen category.

### 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 January 2012 through January 2017. The objectives of the audit were to determine if the: (1) LASD Laboratory was in compliance with select National DNA Index System (NDIS) Operational Procedures; (2) LASD Laboratory was in compliance with certain Quality Assurance Standards (QAS) issued by the FBI; and (3) LASD 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 LASD Laboratory QAS review reports and supporting documentation for corrective action taken, if any, to determine whether: (a) the LASD 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 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 LASD Laboratory officials to identify management controls, LASD Laboratory operational policies and procedures, LASD Laboratory certifications or accreditations, and analytical information related to DNA profiles.
- Toured the LASD Laboratory to observe facility security measures as well as the procedures and controls related to the receipt, processing, analyzing, and storage of forensic evidence and convicted offender DNA samples.
- Reviewed the LASD 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 142 NDIS matches to determine whether they were resolved in a timely manner. The sample was judgmentally

selected to include both case-to-case matches and case-to-offender matches. This non-statistical sample does not allow projection of the test results to all matches.

- Reviewed supporting documentation to determine whether the LASD Laboratory provided adequate vendor oversight.
- 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 5,639 searchable forensic profiles the LASD Laboratory had uploaded to NDIS as of January 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 LASD 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 LASD 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 Participation Requirements

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 Procedures:

- NDIS Laboratories
- Quality Assurance Standards Audit Review
- NDIS Confirmation and Hit Dispositioning
- NDIS DNA Records
- NDIS DNA 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 LASD 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.

- Sample Control (Offender QAS 7.1 and 7.2): The laboratory shall have and follow a documented sample inventory control system to ensure the integrity of the database and known samples. Where possible, the laboratory shall retain the database sample for retesting for quality assurance and sample confirmation purposes.
- 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 are reasonable and within the constraints of scientific knowledge.

(Offender QAS Standard 12.1): The laboratory shall have and follow written procedures for reviewing DNA records and DNA database information, including the resolution of database matches.

- [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 review 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 and Offender QAS Standard 17.1): 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.
- Offender QAS Standard 17.4: An NDIS participating laboratory shall have, follow and document appropriate quality assurance procedures to verify the integrity of the data received from the vendor laboratory including, but not limited to, the following: Random reanalysis of database, known or casework reference samples; Inclusion of QC samples; Performance of an on-site visit by an NDIS participating laboratory or multi-laboratory system outsourcing DNA sample(s) to a vendor laboratory or accepting ownership 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 analyst 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 crime.

LABORATORY'S RESPONSE TO THE DRAFT AUDIT REPORT



OFFICE OF THE SHERIFF

COUNTY OF LOS ANGELES

HALL OF JUSTICE

JIM McDONNELL, SHERIFF



September 11, 2017

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

Dear Mr. Gaschke:

This letter contains our official response to the Draft Audit Report of the Department of Justice Office of the Inspector General (OIG), titled AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE LOS ANGELES COUNTY SHERIFF'S DEPARTMENT SCIENTIFIC SERVICES BUREAU CRIME LABORATORY LOS ANGELES, CALIFORNIA, dated September 1, 2017. The audit was performed to determine if the: (1) Laboratory is in compliance with select National DNA Index System (NDIS) Operational Procedures; (2) Laboratory is in compliance with certain quality assurance standards issued by the Federal Bureau of Investigation; and (3) Laboratory's forensic DNA profiles in Combined DNA Index System (CODIS) databases are complete, accurate, and allowable for inclusion in NDIS.

We do question the accuracy of some of the statements in the draft audit report.

**Page ii** – "The LASD Laboratory did not limit and control access to its laboratory as required by NDIS's Security Requirements. Specifically, we found that there were former employees who had retained active keycards to restricted areas of the LASD Laboratory after their employment with the LASD had ceased. We also found keycards assigned to unknown individuals and individuals with inappropriate access to restricted areas of the LASD Laboratory."

**Response:** This statement is repeated in various areas of the report, however, the audit did not find any evidence that any former employees retained active keycards. It is true that our policy to have the employee sign on the physical log in the Facility Manager's office when returning the card, and for the staff of the Facility Manager to deactivate the cards upon receipt was not followed 100% of the time, which we have remedied, but that does not mean that the cards were not collected. Additionally, the audit found no

211 WEST TEMPLE STREET, LOS ANGELES, CALIFORNIA 90012

*A Tradition of Service*  
— Since 1850 —

evidence that any former employee ever used a keycard to enter the building, the fourth floor, or the CODIS room at any time following their separation of employment.

**Page ii** – “We found more than 550 individuals had access to the fourth floor space where a client terminal was located, including former LASD employees (one of which also had access to the CODIS server room) and individuals whose employers we could not determine. We also determined that the LASD Laboratory did not have adequate security measures in place to protect against unauthorized personnel gaining access to DNA records or data. Specifically, we found CODIS specimen reports that were left next to a CODIS terminal located in a cubicle in the common area of the fourth floor.”

**Response:** This statement is repeated in various areas of the report, however, all individuals who had access via keycard have been background checked and are trusted employees. There are no individuals on the list that was provided to the auditors whose employers are not known and who have not been given authorization by me or the Laboratory Director of the Los Angeles Police Department Crime Lab to be in those areas.

**Page ii** – “we found 9 forensic profiles that were uploaded to CODIS prior to receiving a secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category, as required by the FBI.”

**Response:** This statement is repeated in various areas of the report, however, we provided clear documentation to the audit team that all proper reviews had been completed prior to being uploaded as required by the FBI.

**Recommendation 1** – “Ensure that it implements the required physical access controls to properly track and maintain its distribution of keycards to ensure that all former employee’s keycards have been deactivated.”

**Response: We disagree.** We already have these security measures in place. We do agree that the key assignment is complicated due to the structure of the tenancy of the building which was designed to house the Los Angeles Sheriff’s Department laboratory, the Los Angeles Police Department laboratory, the California State University Los Angeles’ Criminal Justice and Criminalistics programs, and the California Criminalistics Institute. (The latter two occupants are housed outside of the laboratory area in the non-secure “university” portion of the building.) But we believe there is still adequate security to the laboratory in spite of the complexity. Several of the personnel that the OIG auditors alluded to in their report have access only to the university portion of the building, which includes lecture rooms, teaching labs, and university offices, but not the laboratory area. To enter the laboratory portion of the building, a person must go through a combination of two secure doors in which proper key card access is required, and then take an elevator to reach the analytical laboratory space. The elevators also require key card access to go to any of the additional floors in the building.

**Recommendation 2** – “Ensure that all individuals (including LASD personnel, contractors, and volunteers) have appropriate access to the fourth floor, areas within the LASD Laboratory, and to the LASD Laboratory’s assets.”

**Response: We disagree.** We already have these security measures in place. The university portion of the building is open to the public during normal business hours, but the laboratory access, which is controlled by armed Sheriff Personnel during business hours, requires key card access or escorts for those who have not been issued key cards. When an employee leaves or changes assignments their key card is taken back and the key card is secured until our facility personnel have time to deactivate it. If an employee does not return the key card, or a key card is lost, it is deactivated, and since the key cards have no identifying information to indicate they are for the Crime Lab facility there is nothing to indicate to someone finding it where it could be used to gain entry. The key card access system was designed so that security can be maintained regardless of whether a key card is returned upon reassignment or employment termination or not.

One of the examples the OIG auditors used as “Inappropriate Access” was a Sheriff’s Department Plumber. All personnel who maintain the facility are Sheriff’s Employees and undergo a lengthy and detailed background investigation (including having their fingerprints checked via local, state, and federal databases as a condition of employment) just as the laboratory staff are screened. The Laboratory Director has specifically authorized some of the facility staff to have access to the labs and offices 24/7 for emergency response so that facility malfunctions can be addressed immediately to reduce the risk of damaging evidence or analytical equipment. For example, the building has its heating/cooling pipes in the gap above the ceiling panels and if a pipe or valve were to leak, any delay caused by requiring a laboratory staff member had to respond first to allow the facility staff into the building could make the situation much worse.

**Recommendation 3** – “Ensure that the distribution of all keycards are properly documented and limited to personnel designated by laboratory management, including performing a review of all unknown keycards and deactivating duplicate keycards.”

**Response: We disagree.** These security measures are already in place. The audit did reveal that in a small number of cases the policy had not been followed, and that has been remedied. As explained to the OIG auditors, the lab is going through a process of changing to newer key cards. Many of the Sheriff’s and LAPD staff have two cards; one is the originally issued card (with corresponding records of issuance), and the second is the newer card. The records of issuance for both cards are maintained by the Facility Manager. These new cards have been in the process of being created and, except for a few exceptions that meet a business need, each employee will be required to turn in

the old access cards as soon as the new card has been verified to work as designed. This transition is ongoing until complete.

**Recommendation 4** – “Ensure that the LASD Laboratory strengthen physical security over the CODIS server and client terminals against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.”

**Response: We disagree.** The physical security is sufficient so that only authorized people have access to the CODIS server and terminals. The location of one CODIS Client Work Stations is at a designated area on the 4<sup>th</sup> floor of the building. The work station has the required security requirements to include CODIS Username/Password sign-on and is set for a 10 minute auto sign-off if idle. Only designated DNA personnel have the required Username/Password credentials. Without those credentials, a person sitting at the CODIS Client Work Station could not access CODIS. Additionally, even if they somehow bypassed the username/password component of the security, they could only enter a profile which would then require a CODIS administrator to actually approve and upload. So with that understanding, we believe it is unreasonable to suggest that someone having access to the work station could compromise CODIS.

The audit did not find any evidence or objective proof that the security of the Client Work Station has ever been compromised, was attempted to be compromised, or that the security could even reasonably be compromised. Additionally, there has been no proof offered by the OIG auditors that there has been any unauthorized or suspect access to any secure laboratory area.

**Recommendation 5** – “Ensure that the LASD Laboratory has adequate physical security measures in place to protect against unauthorized personnel gaining access to any DNA records or data.”

**Response: We disagree.** All individuals who had access via keycard have been background checked and are trusted employees. There are no individuals on the list that was provided to the auditors whose employers are not know and who have not been given authorization by me or the Laboratory Director of the Los Angeles Police Department Crime Lab to be in those areas. All visitors are escorted unless they are background-checked employees of either department. Whether any records or data are temporarily left out, they are always secured in an area where there are only authorized people who have access.

**Recommendation 6** – “Ensure that the LASD Laboratory adequately performs its internal QAS reviews to verify compliance with each QAS, including ensuring that the distribution of all keycards are current, accurate, clearly documented, and available for review.”

**Response: We disagree.** The DNA section has gone through external assessments in 2012, 2014, 2015 and 2017, as well as an FBI/NDIS assessment in May 2014, and there were no findings related to any of the recommendations listed in the report. All

auditors involved in each of these audits have received specific auditing training that conforms to the internationally recognized ISO 19011 Standard entitled Guidelines for Auditing Management Systems and also gives specific information on auditing to the FBI QAS standards. ISO 19011 is the standard for auditing within the world of Quality Assurance.

As far as the keycard security goes, the audit did reveal that in a small number of cases the policy had not been followed, and that has been remedied. The policy is otherwise sufficient, and in that regard the audit has been helpful.

**Recommendation 7** – “Ensure that all case files contain sufficient information in order to determine CODIS eligibility.”

**Response: We disagree.** All of our current case files do contain sufficient information in order to determine CODIS eligibility, and that has been the case since the FBI/NDIS audit of May 2014. Some of the 16 profiles mentioned in the draft report were entered before May 2014. Based on one of the action items of that audit, the lab requires more detailed information about CODIS eligibility. As stated during the audit, prior to the May 2014 FBI/NDIS audit the lab relied on the Law Enforcement Agencies (LEA's) answer “YES” to the following question on our CHECK-PC collection kit: *“Based on the case history, is this evidence attributable to the suspect of the crime? [i.e. could NOT have come from a resident (victim) or person(s) known to frequent the crime scene.]”*

During the audit, the lab contacted the Law Enforcement Agencies (LEAs) for the 16 cases which came into question. Additional details were obtained to satisfy the auditor's review of CODIS eligibility. The comments about Sample number 27 are a misrepresentation of the facts. This was a 2011 case submission. At the request of the auditors, the CODIS Administrator contacted the current CHOP Coordinator for the LEA, not the original investigating officer. The CHOP coordinator located the case information and felt that it may not be eligible. At no time did the CODIS Administrator state he was in contact with the investigating officer that made the original submission. The submission envelope from the BODE SecurSwab Collection kit indicated “YES” to the collection kit eligibility question. As stated above, since the May 2014 audit the lab no longer solely relies on a “YES” to the eligibility question on the above mentioned collection kit.

The auditors recommended that “like other labs” we should consider including the crime report in the case file. We have two concerns about this. First, based on the number of different LEAs our lab services, this recommendation is not practical. Police Department and Sheriff Station/Bureaus use different reporting processes that may not be compatible with the labs LIMS system. Additionally, suggesting that we be “like other labs” is inappropriate, and it takes the audit away from basing our compliance/non-compliance on the FBI standards. According to Section 4 of ISO 19011 (paraphrased), the principles of auditing require the auditors to be independent,

impartial, and free from bias. This gives us the perception that the audit has strayed from the statement in Appendix 1, where it says "We conducted this performance audit in accordance with generally accepted government auditing standards."

**Recommendation 8** – "Ensure that all DNA profiles prior to being uploaded into CODIS receive a concordant assessment for CODIS eligibility, correct DNA types, and the appropriate specimen category."

**Response: We disagree.** Although we strive for perfection, out of a total of 116 profiles examined during the audit, only one allele from the entire profile was entered in incorrectly. The locus was D21S11 and the alleles entered were 29, 31.2 and should have been 29, 32.2. With potentially 16 loci from each of the 116 profiles examined (116 profiles x 16 loci x 2 allele/locus), and potentially 3,712 alleles entered, that would equate to 99.973% accuracy or a 0.027% inaccuracy for entering alleles. Although we have developed a quality assurance program to catch nearly all inaccuracies that may happen, there is another safety net since CODIS at the State and NDIS level conducts special searches to catch this infrequently occurring error that can occur with a miss entry for one locus.

During our exit telephone conference call three days before the issuance of their draft, the auditors announced for the first time that they believed there were twenty-seven profiles that did not go through the CODIS verification before upload, in particular, they had not had a required "technical review." During the call, the CODIS Administrator explained that the lab only uploads a specimen after it has gone through a documented CODIS Verification by two qualified analysts. He explained that the CODIS Verification, which includes all the requirements outlined in the FBI/QAS and NDIS Procedures, is documented on the Specimen Detail Report form and includes two qualified analyst's initials, the date, and the word "verified" on the report print out. The CODIS Administrator also explained to the auditors that the CODIS Verification is different than the "Technical Review," and that it can occur prior to the final report's Technical Review. The auditors stated that "other labs" do the CODIS Verification as part of the Technical Review, which we believe is irrelevant and should not be considered as a part of an audit. We explained again that neither the FBI QAS standards nor the NDIS operating requirements require that the CODIS verification be conducted at the same time as the technical review, or be included in the technical review, as long as all requirements for each review are met.

At the request of the laboratory, the auditors provided the laboratory with the specimen numbers that were in question. In spite of the short notice given to the lab of the perceived shortcoming, the auditors stated they would remove the recommendation from the report only if the CODIS Administrator could provide proof of CODIS Verification by the next day. That documentation was provided the next day as requested which showed the date of the CODIS verification to be on or before the date they were uploaded to State DNA Index System (SDIS) for all twenty-seven specimens.

The laboratory then received a final list of nine specimens the auditors felt were not verified. Seven were from the twenty-seven mentioned above and two more had been added. Documentation of CODIS verification for all nine were again sent to the auditors showing that the CODIS verification occurred prior to being uploaded. With respect to these nine samples and the auditors' incorrect interpretation that those profiles were uploaded without the proper verification, the laboratory assumes that the auditors inadvertently referred to the "Specimen Verification Form" instead of the "Specimen Detail Report" in arriving at that conclusion. As was explained to the auditors on more than one occasion, the Specimen Verification Form is not used to document that CODIS Verification, but it is only used by the reviewer as a tool to ensure he or she has completed all the verification steps.

**General Response Relative to the Audit:**

The laboratory is generally concerned about the ability of the OIG auditors to properly assess a forensic laboratory. If, as an auditor stated in the closing teleconference, the auditors followed "standard auditing principles," each of the principles found in section 4 of ISO 19011 should have been followed. Our responses have elucidated numerous instances of these principles not being followed. Not the least of which is the responsibility of the auditors to audit strictly to the requirements in question, which are NDIS operating requirements and FBI QAS standards, and to not audit to an irrelevant and undefined standard of "what other laboratories do."

Sincerely,

JIM McDONNELL, SHERIFF



Wesley P. Grose  
Laboratory Director



Steve Renteria  
CODIS Administrator



THE FBI'S RESPONSE TO THE DRAFT AUDIT REPORT



U.S. Department of Justice  
Federal Bureau of Investigation

---

Washington, D.C. 20535-0001

September 15, 2017

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

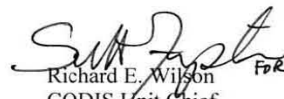
Dear Mr. Gaschke:

Your memorandum, to Director Wray, forwarding the draft audit report for the Los Angeles County Sheriff's Department Scientific Services Bureau Crime Laboratory, Los Angeles, California ("Laboratory"), has been referred to me for response.

Your draft audit report contained eight recommendations relating to the Laboratory's compliance with the FBI's Memorandum of Understanding (MOU) and *Quality Assurance Standards for Forensic DNA Testing Laboratories (QAS)*. As noted in the draft report, compliance with the MOU and the QAS is required for forensic laboratories participating in the National DNA Index System. The FBI CODIS Unit has reviewed and agrees with the recommendations to the Laboratory. Accordingly, the CODIS Unit is in contact with the Laboratory and is working with its staff to ensure that the Laboratory creates a plan and implements procedures to address each recommendation. The CODIS Unit will monitor the Laboratory's progress.

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 REPORT**

The Office of the Inspector General (OIG) provided a draft of this audit report to the LASD Laboratory and FBI for review and official comment. The responses from the LASD Laboratory and FBI are incorporated in Appendices 3 and 4, respectively, of this final report. In response to our draft audit report, the FBI concurred with our recommendations and discussed the actions it plans to complete in order to address the recommendations. As a result, the report is resolved. The LASD Laboratory disagreed with each of our eight recommendations, as discussed below. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

**Analysis of the LASD Laboratory's Response**

In response to our audit, the LASD Laboratory questioned the accuracy of some of the statements in the draft audit report. We address each of the LASD Laboratory's statements below.

The first statement in the report that the LASD Laboratory took exception to was the following:

The LASD Laboratory did not limit and control access to its laboratory as required by NDIS's Security Requirements. Specifically, we found that there were former employees who had retained active keycards to restricted areas of the LASD Laboratory after their employment with the LASD had ceased. We also found keycards assigned to unknown individuals and individuals with inappropriate access to restricted areas of the LASD Laboratory.

The LASD Laboratory stated that the audit did not find any evidence that any former employees had retained active keycards. We disagree. On August 4, 2017, the Laboratory provided us documentation of the Hertzberg-Davis Forensic Science Center Access Card/Key(s) Request Form (keycard request form) for each of the eight former LASD employees. On each of the keycard request forms it stated, ". . . employee no longer works in building. Card not returned." and the form was initialed and dated by the LASD's Facility Manager's Assistant. The eight keycards were listed as active on the keycard distribution list provided by the LASD Laboratory. The LASD Laboratory in its response, stated that the audit found no evidence that any former employee used a keycard to enter the building, the fourth floor, or the CODIS room at any time following their separation of employment. However, our audit testing did not include a review of whether or not the eight former employees inappropriately accessed the LASD Laboratory after they ceased working for the LASD. We did review the LASD Laboratory's keycard distribution

list, as required by the FBI's QAS Standard 6, to determine if the distribution system of all keys and combinations were current, accurate, and clearly documented, and available for review. We determined that the list contained inaccuracies and was not current as former employees had not returned active keycards, keycards were assigned to unknown individuals, and individuals had inappropriate access to restricted areas of the LASD Laboratory. Further, based on these findings, we identified that the LASD Laboratory was in violation of the FBI's NDIS Security Requirements, requiring that NDIS participating laboratories have controlled access to its laboratory and laboratory assets. In our report, we state that by not maintaining a current and accurate list of active keycards, the LASD Laboratory increases the risk that both information and evidence may be inappropriately accessed or mishandled and compromises the security of the Laboratory, as well as the privacy right of individuals whose information is maintained by the Laboratory.

The next statement in the report that the LASD Laboratory took exception to was the following:

We found more than 550 individuals had access to the fourth floor space where a client terminal was located, including former LASD employees (one of which also had access to the CODIS server room) and individuals whose employers we could not determine. We also determined that the LASD Laboratory did not have adequate security measures in place to protect against unauthorized personnel gaining access to DNA records or data. Specifically, we found CODIS specimen reports that were left next to a CODIS terminal located in a cubicle in the common areas of the fourth floor.

The LASD Laboratory stated that all individuals who had access via keycard have been background checked and are trusted employees. We do not make any assertions in our report related to employees having or not having undergone LASD background checks, and we do not make assumptions concerning the Laboratory's trust in its employees. However, the NDIS Security Requirements state that NDIS participating laboratories 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. Therefore, based on the security risks we have identified, including: (1) former personnel having had active keycards; (2) LASD personnel with inappropriate access to the fourth floor and restricted areas of the laboratory, and (3) more than 550 individuals with access to where a client terminal was located and a DNA specimen report was left out; we found that the Laboratory is not in compliance with the FBI's NDIS Security Requirements and unnecessarily assumes a serious risk of unauthorized access to the LASD Laboratory.

The LASD Laboratory also stated that there are no individuals on the list who were provided to the auditors whose employers are unknown and who have not been given authorization by either the LASD Laboratory Director or the LAPD Laboratory Director to be in those areas. We disagree. During our fieldwork, we received a keycard distribution list that included 877 active keycards having access

to the fourth floor, where the LASD Laboratory is located. Based on our review of the distribution list, we were unable to determine to whom 49 of the keycards were issued. Although the LASD Laboratory stated in its response that it knows who each of the 49 keycards belongs to and that it properly approved each keycard, the LASD Laboratory did not provide documentation to support its statement either during our audit or with its response to our draft report. In addition, regardless of whether the identity of each individual provided access to these areas is known, the NDIS QAS specifically states that the distribution system of all keys and combinations are required to be current, accurate, clearly documented, and available for review. During our fieldwork the LASD Laboratory failed to provide an accurate and current listing of its keycard distribution list. Therefore, the LASD Laboratory was not in compliance with the FBI's QAS.

The next statement in the report that the LASD Laboratory took exception to was the following:

"In addition, we found 9 forensic profiles that were uploaded to CODIS prior to receiving a secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category, as required by the FBI."

The LASD Laboratory stated that it had provided clear documentation to the audit team that all proper reviews had been completed prior to being uploaded as required by the FBI. We reviewed the documentation provided to us after the exit conference, and we discuss this matter further in Recommendation 8, below.

Lastly, the LASD Laboratory stated in its response that it was "generally concerned about the ability of the OIG auditors to properly assess a forensic laboratory." The LASD Laboratory response goes on to state that OIG auditors should have followed "the principles found in section 4 of ISO 19011" and claims "that [the LASD Laboratory] responses have elucidated numerous instances of these principles not being followed." We disagree with the LASD Laboratory's assertions for several reasons. First, for the reasons discussed in this Appendix, we disagree with the specific claims made in the LASD Laboratory response about our audit findings, which are fully supported by our fieldwork and are consistent with the principles in section 4 of ISO 19011. Second, the OIG auditors who performed this audit underwent CODIS-specific training and consulted with the FBI during the course of the audit regarding our findings. Third, while the LASD Laboratory claims that the OIG did not strictly audit to the requirements of the FBI's QAS, the FBI agreed with all of our recommendations related to the LASD Laboratory's compliance with the standards governing CODIS and stated that it would work with the LASD Laboratory to address the recommendations. Lastly, our audit was conducted in accordance with generally accepted government auditing standards, with the conclusions and findings in the report based on evidence obtained during the audit.

## Recommendations for the FBI :

1. **Ensure that it implements the required physical access controls to properly track and maintain its distribution of keycards to ensure that all former employee's keycards have been deactivated.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the LASD Laboratory to correct this finding.

The LASD Laboratory stated in its response that it did not agree with our recommendation and that it already has security measures in place. We disagree that its measures in place are adequate. Our audit found that eight former LASD employees had retained active keycards with access to the fourth floor and to restricted areas of the Laboratories after their employment with the LASD had ceased. Therefore, the LASD Laboratory did not have adequate physical security controls in place to ensure that it properly collected and deactivated keycards when employees departed the LASD Laboratory. In its response, the LASD Laboratory also stated that several of the personnel that the OIG auditors alluded to in their report have access only to the university portion of the building, which includes lecture rooms, teaching labs, and university offices, but not to the laboratory area. However, based on our review of the LASD Laboratory's keycard distribution list, we found more than 550 individuals had access to the fourth floor space where a CODIS client terminal was located, including former LASD employees (one of which also had access to the CODIS server room) and individuals whose employers we could not determine.

This recommendation can be closed when we receive evidence that the LASD Laboratory has implemented the required physical access controls to properly track and maintain its distribution of keycards to ensure that all former employee's keycards have been deactivated.

2. **Ensure that all individuals (including LASD personnel, contractors, and volunteers) have appropriate access to the fourth floor, areas within the LASD Laboratory, and to the LASD Laboratory's assets.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the LASD Laboratory to correct this finding.

The LASD Laboratory stated in its response that it did not agree with our recommendation and that it already has security measures in place. The LASD Laboratory stated that the university portion of the building is open to the public during normal business hours, but the laboratory access, which is controlled by armed Sheriff personnel during business hours, requires keycard access or escorts for those who have not been issued key cards. Its response further stated that when an employee leaves or changes assignments, their keycard is taken back and the keycard is secured until our facility personnel have time to deactivate it. The LASD Laboratory also

stated that if an employee does not return the keycard or a keycard is lost, it is deactivated.

We disagree with the LASD Laboratory's statement that if an employee does not return a keycard that the keycard is deactivated. As stated in our report, we found eight former LASD employees had not returned active keycards with access to the fourth floor and to restricted areas of the Laboratories after their employment with the LASD had ceased. Specifically, we found five of the former employees held active keycards for 11 months or more after ceasing employment with the LASD Laboratory; the lengthiest example was a keycard that remained active approximately 2.5 years after the employee's departure. The LASD Laboratory stated its keycard access system was designed so that security can be maintained regardless of whether a keycard is returned upon reassignment or employment termination or not. Without ensuring that all employees who no longer require keycard access have had their keycards properly collected and deactivated, the LASD Laboratory increases the risk that both information and evidence may be inappropriately accessed or mishandled and compromises the security of the Laboratory, as well as the privacy rights of individuals whose information is maintained by the Laboratory.

In its response, the LASD Laboratory also stated that all LASD employees, including a LASD plumber mentioned in the OIG report, undergo a lengthy background check the same as LASD Laboratory staff. The Laboratory Director has specifically authorized some of its facilities staff to have access to the Laboratory and offices 24 hours a day for emergency response so that facility malfunctions can be addressed immediately to reduce the risk of damaging evidence or analytical equipment. For example, the building has its heating and cooling pipes in a gap above the ceiling panels and if a pipe or valve were to leak, any delay caused by requiring a Laboratory staff member having to respond first to allow the facilities staff into the building could make the situation worse. We found that a plumber had access to the evidence exam room, where, based on LASD Laboratory policy, evidence is allowed to be left out until the end of the work day, at which time the evidence is required to be secured. According to NDIS Security Requirements, NDIS participating laboratories are required to have adequate physical security measures in place to protect against unauthorized personnel gaining access to DNA samples or any DNA data. During our audit, the LASD Laboratory agreed that the plumber should not have access to this area and restricted the plumber's access to the exam room. As a result of our audit, the LASD Laboratory restricted access rights to 43 individuals that had been provided access to areas of the LASD Laboratory that were not required in order to perform their job responsibilities.

This recommendation can be closed when the LASD Laboratory has ensured that only appropriately cleared individuals and active employees have access to the fourth floor, including areas within the LASD Laboratory and to the LASD Laboratory's assets.

3. **Ensure that the distribution of all keycards are properly documented and limited to personnel designated by laboratory management, including performing a review of all unknown keycards and deactivating duplicate keycards.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the LASD Laboratory to correct this finding.

The LASD Laboratory stated in its response that it did not agree with our recommendation and that it already has security measures in place. The LASD Laboratory stated that although the audit did reveal in a small number of cases where the policy had not been followed, those cases had been remedied. In its response, the LASD Laboratory stated that it is going through a process of changing to newer keycards, whereby each employee, with a few exceptions, will be required to turn in the old access cards as soon as the new card has been verified to work as designed. The LASD Laboratory stated that the transition is on-going. In our report, we determined that 214 of the 877 active keycards (24 percent) were assigned to individuals in duplicate. Out of the 214 keycards issued to individuals in duplicate, 28 were assigned to 24 LASD Laboratory employees. We also were unable to determine to whom 49 keycards were issued. Providing keycards to individuals without properly documenting to whom the keycards were assigned and assigning cards in duplicate to employees increases the risk of loss and theft of a keycard while at the same time weakening controls that could prevent unauthorized access to the Laboratory, including restricted areas within the Laboratory.

This recommendation can be closed when we receive evidence that the distribution of all keycards are properly documented and limited to personnel designated by laboratory management, including an appropriate determination for all unknown keycards and the deactivation of duplicate keycards.

4. **Ensure that the LASD Laboratory strengthen physical security over the CODIS server and client terminals against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the LASD Laboratory to correct this finding.

The LASD Laboratory stated in its response that it did not agree with our recommendation and that its physical security is sufficient so that only authorized individuals have access to the CODIS server and client terminals. We disagree with the LASD Laboratory's statement because we found that one former employee that no longer work at the LASD Laboratory had keycard access to the CODIS server room for approximately 2.5 years after

their employment with the LASD Laboratory had ended. We also found that a CODIS client terminal was located in the cubicle space in the common area of the fourth floor. According to the FBI's QAS, access to the laboratory shall be controlled and limited in a manner to prevent access by unauthorized personnel. Additionally, the LASD Laboratory is required to ensure that it has adequate physical security measures in place to protect against unauthorized personnel gaining access to DNA samples or any DNA data. In its response, the LASD Laboratory stated that the client terminal has the required security requirements and that it is unreasonable to suggest that someone having access to the work station could compromise CODIS. We disagree with the LASD Laboratory's statement because, as previously discussed, we believe that access to the LASD Laboratory was not limited and controlled as required by NDIS's Security Requirements. The fact that the keycard access system is shared with another agency (LAPD Laboratory) indicates that the LASD Laboratory does not have exclusive control over who has access to its space on the fourth floor. Further, as mentioned before, we found weaknesses with the LASD Laboratory's controls over keycards that were improperly assigned to former LASD Laboratory employees, unknown individuals, and unauthorized individuals allowing such individuals access to the fourth floor of the LASD Laboratory. Based on the issues we have identified, we believe that there is serious risk of unauthorized access to the LASD Laboratory and the client terminal located in the common area of the fourth floor. The LASD Laboratory stated that the audit did not find any evidence that the security of the client work station has ever been compromised, was attempted to be compromised, or that the security on it even could be compromised. Our audit testing did not include a review of whether or not the CODIS client terminal had been inappropriately accessed, and therefore, we do not make any assertions in our report related to inappropriate electronic access of the LASD Laboratory's CODIS client terminals.

This recommendation can be closed when we receive evidence that the LASD Laboratory has strengthened physical security over the CODIS server and client terminals against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

**5. Ensure that the LASD Laboratory has adequate physical security measures in place to protect against unauthorized personnel gaining access to any DNA records or data.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the LASD Laboratory to correct this finding.

The LASD Laboratory stated in its response that it did not agree with our recommendation and that all individuals who had keycard access had gone through background checks and were trusted employees. Our audit testing did not include a review of the adequacy of the LASD's background investigation process and therefore, we did not make any assertions



regarding it in our report. The LASD Laboratory also stated that all employees had been given access authorization by the LASD or LAPD Laboratory Directors and that any records or data temporarily left out were only done so in an area secured and accessible by authorized people. However, as we discussed in our audit report, more than 550 individuals had access to the fourth floor space where a client terminal was located with a specimen detail report sitting next to it, including former LASD and LAPD employees as well as individuals whose employers we could not determine.

This recommendation can be closed when we receive evidence that the LASD Laboratory has adequate physical security measures in place to protect against unauthorized personnel gaining access to any DNA records or data.

**6. Ensure that the LASD Laboratory adequately performs its internal QAS reviews to verify compliance with each QAS, including ensuring that the distribution of all keycards are current, accurate, clearly documented, and available for review.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the LASD Laboratory to correct this finding.

The LASD Laboratory stated in its response that it did not agree with our recommendation and that none of its external reviews in 2012, 2014, 2015, and 2017 noted any findings relating to any of the recommendations listed in the OIG report. The LASD Laboratory agreed that our audit was helpful in revealing a small number of instances where its keycard security policy had not been followed and that those instances have been remedied. The LASD Laboratory stated that its policy is otherwise sufficient. We disagree with the LASD Laboratory's statement because we found several instances where the LASD Laboratory was not in compliance with both the FBI's NDIS Security Requirements and the QAS. For example, we found that the LASD Laboratory, by allowing former employees access to restricted areas of the Laboratory, was in violation of the FBI's NDIS Security Requirement, requiring that NDIS participating laboratories have controlled access to its laboratory and laboratory assets. Additionally, according to the FBI's QAS Standard 6, the laboratory must demonstrate compliance which includes ensuring that the distribution system of all keys and combinations are current, accurate, clearly documented, and available for review. The LASD Laboratory's keycard distribution list was outdated and inaccurate as former personnel had active keycards (one former employee since November 2014), unknown individuals had been assigned keycards, and individuals had inappropriate keycard access to areas of the Laboratory. The LASD Laboratory has not yet remedied all of the OIG findings relating to its keycard access distribution system. The LASD Laboratory's policy also requires that issued keycards be verified during the annual QAS review. Based on the security risks we identified during our audit and the fact that both the internal and external QAS reviews failed to detect the LASD Laboratory's security issues, we believe that the LASD Laboratory's internal

QAS review can be improved, in particular with regard to ensuring the LASD Laboratory's adherence to QAS Standard 6. To rectify the deficiencies we identified, the LASD Laboratory should establish controls over its internal QAS reviews to ensure the reviews are performed to identify whether the distribution of all keycards are current, accurate, clearly documented, and available for review. In addition, the LASD Laboratory should review the entire keycard distribution list rather than just a sample of keycards and ensure that all keycard holders that have been granted access rights still require those access rights.

This recommendation can be closed when we receive evidence that the LASD Laboratory will adequately perform its internal QAS reviews to verify compliance with each QAS, including ensuring that the distribution of all keycards are current, accurate, clearly documented, and available for review.

**7. Ensure that all case files contain sufficient information in order to determine CODIS eligibility.**

Resolved. The FBI concurred with our recommendation and stated that it will work with the LASD Laboratory to correct this finding.

The LASD Laboratory stated in its response that it did not agree with our recommendation and that all of its case files uploaded to CODIS after May 2014, contain sufficient information in order to determine CODIS eligibility. The LASD Laboratory further stated that the FBI conducted a NDIS review of the LASD Laboratory in May 2014, which resulted in an action item that the Laboratory require more detailed information about CODIS eligibility. In its response to our draft report, the LASD Laboratory stated that it used to rely on law enforcement agencies (LEA) answering "Yes" to the following question on its CHECK-PC collection kit: "Based on the case history, is the evidence attributable to the suspect of the crime?" During our fieldwork, the CODIS Administrator stated that if the LEA circled "Yes" then the DNA Analyst would determine if the profile is eligible for CODIS without any documentation to determine if a crime was committed, what type of crime had occurred, and if the evidence was attributable to a putative perpetrator. The LASD Laboratory took corrective action by informing all DNA Analysts that supporting documentation was required when determining CODIS eligibility.

In its response, the LASD Laboratory stated that some of the 16 profiles identified in the OIG report as not containing sufficient information in order to determine CODIS eligibility were uploaded to CODIS prior to May 2014. However, our audit also found that 3 of the 16 forensic profiles that lacked sufficient information to determine CODIS eligible were uploaded to CODIS after the FBI's May 2014 review. For each of the 16 forensic profiles, the LASD Laboratory had to reach out to the LEA to obtain additional information regarding the crime or the evidence. Based on the LEA's information, we determined that 15 of the profiles were eligible for upload into NDIS and that 1 profile, Sample Item 27, was determined not to be eligible and was

removed from CODIS. The LASD Laboratory stated that Sample Item 27 was a 2011 case submission and that the OIG's comments about the sample were a misrepresentation of the facts. The LASD Laboratory stated that the CODIS Administrator contacted the current LEA and not the original investigating officer as stated in the OIG report. The LASD Laboratory response further states that the submission envelope from its CHECK-PC collection kit indicated "Yes," that based on the case history, the evidence was attributable to the suspect of the crime. The LASD Laboratory stated that it no longer accepts "Yes" circled on the collection kit as sufficient information to determine CODIS eligibility and therefore, does not rely on the collection kit indicating "Yes" alone and obtains additional documentation to determine if the forensic profile is eligible for upload into NDIS. We updated the report to reflect the new information provided by the LASD Laboratory pertaining to the title of the individual from whom the Laboratory received information regarding Sample Item 27 during our audit.

The LASD Laboratory also stated that the auditors recommended that "like other labs" we should consider including the crime report in the case file. The LASD Laboratory stated that based on the number of different LEAs that it services that is not practical and that LEAs use different reporting processes that may not be compatible with its Property and Evidence Information Management System. The LASD Laboratory stated that it is inappropriate for OIG auditors to suggest they be "like other labs" and took the audit away from the laboratory's compliance with the FBI's standards and gave the perception that the audit was not conducted in accordance with generally accepted government auditing standards. We disagree with the LASD Laboratory's statement for several reasons. First, we did not prescribe any specific action for the LASD Laboratory to remedy the findings we have identified. The decision of how to remedy a finding is left to the discretion of the auditee, with the concurrence of the FBI as to the correct plan of action that needs to be implemented for the remediation of all findings. Additionally, based on the generally accepted government auditing standards, routine activities performed by auditors that relate directly to the performance of an audit include providing information to the audited entity that is readily available to the auditor, such as best practices and benchmarking studies. Providing an auditee, such as the LASD Laboratory, information about best practices is well within the audit's purview, is in accordance with government auditing standards, and does not affect our independence as the LASD Laboratory indicates. Improvements to the Laboratory's practices, such as the best practices we communicated, may help avoid future instances of the Laboratory's noncompliance with NDIS edibility requirements we revealed during this audit.

This recommendation can be closed when the LASD Laboratory ensures that all case files contain sufficient information in order to determine CODIS eligibility.

**8. Ensure that all DNA profiles prior to being uploaded into CODIS receive a concordant assessment for CODIS eligibility, correct DNA types, and the appropriate specimen category.**

Closed. The FBI concurred with our recommendation, and we consider this recommendation closed based on our review of new information and documentation provided by the LASD Laboratory after our draft report was issued.

The LASD Laboratory stated in its response that it did not agree with our recommendation. In addition, it stated that out of a total of 116 forensic profiles examined during the audit, only one allele was entered incorrectly (Sample Item 38), translating into a 99 percent accuracy rate when accounting for the alleles in each profile. However, the basis for this recommendation was not the inaccurate profile we identified, but rather it was based on the Laboratory's inconsistent explanations for documenting its secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category.<sup>16</sup>

The LASD Laboratory in its response also provided information from the audit closeout meeting (exit conference) that helped address 27 forensic profiles, which we originally questioned because we did not have evidence that they underwent a required technical review. The Laboratory had provided documentation of its technical review for those 27 profiles, and we confirmed with the NDIS custodian that the Laboratory's practices for such documentation was acceptable prior to the issuance of our draft report.

However, as discussed in our draft report, the LASD Laboratory uploaded nine profiles to CODIS without documentation of a prior review for CODIS eligibility, correct DNA types, and the appropriate specimen category, as required by the FBI.<sup>17</sup> During our exit conference, the CODIS Administrator stated that the CODIS Data Verification Form – which documents the review of eligibility, DNA type, and specimen category – is required to be completed in addition to the review conducted and documented on the specimen detail report. After performing additional analysis, we determined that nine profiles did not have such documentation, despite the representation by the Laboratory that it is required to be performed prior to upload to NDIS in

---

<sup>16</sup> We also note that, as detailed in our report, we selected a sample of 100 forensic profiles that the LASD Laboratory had uploaded to NDIS as of January 2017, not 116 as stated by the LASD Laboratory in its response. Also, as stated in the Objective, Scope, and Methodology section of our report, the results obtained from our testing a limited sample of profiles may not be projected to the universe of profiles from which the sample was selected.

<sup>17</sup> As discussed in our report, we also identified one profile that was missing the signature attesting to the completion of the review, and another profile that was missing the date of its secondary review. As discussed later, the Laboratory provided documentation that all profiles were reviewed prior to upload to NDIS.

addition to the initial and secondary review conducted and documented on the specimen detail report.<sup>18</sup> As a result, we concluded in our draft audit report that the Laboratory needed to improve its procedures in this regard.

After the draft report was issued, the LASD Laboratory provided new information indicating that documentation of the LASD Laboratory's initial review of the DNA profile for eligibility, DNA type, and specimen category is evidenced by a second signature on the Specimen Detail Report. The Laboratory represented that the CODIS Data Verification Form it completes, which also documents a review for eligibility, DNA types, and specimen category, is another control to ensure this review is completed, but is not required to be completed prior to upload of the profile to NDIS. As a result, we performed additional analysis of the NDIS record, CODIS Data Verification Form, and the specimen detail report and determined that all of the forensic profiles we reviewed received a secondary review for CODIS eligibility, correct DNA types, and the appropriate specimen category prior to NDIS upload.

Based on our review of the new information and documentation provided by the LASD Laboratory during and after our exit conference, we consider this recommendation closed.

---

<sup>18</sup> Also in its response, the LASD Laboratory indicates that we may have been referring to signatures on the Specimen Verification Form instead of the Specimen Detail Report when performing our analysis. This is incorrect. We were reviewing the signatures on the CODIS Data Verification Form, as identified by the CODIS Administrator. We were not provided Specimen Verification Forms.

*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](http://www.justice.gov/oig/hotline) or (800) 869-4499.*



Office of the Inspector General  
U.S. Department of Justice  
[www.justice.gov/oig](http://www.justice.gov/oig)