



**AUDIT OF  
COMPLIANCE WITH STANDARDS GOVERNING  
COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE  
SAN FRANCISCO POLICE DEPARTMENT  
CRIMINALISTICS LABORATORY  
SAN FRANCISCO, CALIFORNIA**

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

Audit Report GR-90-12-001  
January 2012

**AUDIT OF  
COMPLIANCE WITH STANDARDS GOVERNING  
COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE  
SAN FRANCISCO POLICE DEPARTMENT  
CRIMINALISTICS LABORATORY  
SAN FRANCISCO, CALIFORNIA**

**EXECUTIVE SUMMARY**

The Department of Justice Office of the Inspector General (OIG), Audit Division, has completed an audit of compliance with standards governing Combined DNA Index System (CODIS) activities at the San Francisco Police Department Criminalistics Laboratory, San Francisco, California (SFPD Laboratory).

**Background**

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 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 is used by local laboratories.

---

<sup>1</sup> DNA, or deoxyribonucleic acid, is genetic material found in almost all living cells that contains encoded information necessary for building and maintaining life. Approximately 99.9 percent of human DNA is the same for all people. The differences found in the remaining 0.1 percent allow scientists to develop a unique set of DNA identification characteristics (a DNA profile) for an individual by analyzing a specimen containing DNA.

## OIG Audit Objectives

Our audit generally covered the period from January 2009 through December 2010. The objectives of our audit were to determine if the: (1) SFPD Laboratory was in compliance with the NDIS participation requirements; (2) SFPD Laboratory was in compliance with the Quality Assurance Standards (QAS) issued by the FBI; and (3) SFPD Laboratory's forensic DNA profiles in CODIS databases were complete, accurate, and allowable for inclusion in NDIS.

Our review determined the following:

- The SFPD Laboratory was in compliance with NDIS participation requirements regarding updated training for Laboratory personnel, maintenance of training and qualification records, and timeliness of NDIS matches. However, the Laboratory was not in compliance with NDIS Security Requirements that state server back-ups must be transported off-site on a monthly basis.
- The SFPD Laboratory was in compliance with the QAS regarding completion of periodic internal and external QAS reviews, implementation of corrective actions presented by internal and external reviews, and retention of evidence. However, the SFPD Laboratory was not in compliance with QAS that require access to the laboratory to be controlled and limited in a manner to prevent access by unauthorized personnel.
- We reviewed 100 of the SFPD Laboratory's 935 forensic profiles in NDIS as of December 22, 2010. Of the 100 forensic profiles sampled, we found that 93 profiles were complete, accurate, and allowable for inclusion in NDIS while 7 profiles were unallowable. Specifically, we identified: (1) two profiles that were not allowable for upload because they violated the FBI's 4x4 rule; (2) three profiles that were not allowable because they were obtained from the suspect's person or residence; (3) one profile from an item that was not connected to a crime; and (4) one profile that was deemed unallowable because it did not meet the Laboratory's own minimum eligibility requirement of seven core loci for upload to CODIS.<sup>2</sup> The Laboratory agreed to remove all seven unallowable profiles from NDIS.

---

<sup>2</sup> The "4x4 rule", published by the FBI in September 2003, is a reference to Section 6.4.6 of the NDIS DNA Data Acceptance Standards, which states that forensic mixture DNA profiles submitted to NDIS may have up to four alleles at a maximum of four core loci, provided that the remaining nine core loci have no more than two alleles at each locus.

We made two recommendations to address the SFPD Laboratory's compliance with standards governing CODIS activities, which are discussed in detail in the Findings and Recommendations section of the report. Our audit objectives, scope, and methodology are detailed in Appendix I of the report and the audit criteria are detailed in Appendix II.

We discussed the results of our audit with SFPD Laboratory officials and have included their comments in the report as applicable. In addition, we requested from the SFPD Laboratory and the FBI written responses to a draft of our audit report. We received those responses and they are found in Appendices III and IV, respectively.

# TABLE OF CONTENTS

<b>INTRODUCTION</b> .....	<b>1</b>
Background .....	1
OIG Audit Objectives .....	1
Legal Foundation for CODIS.....	2
CODIS Structure .....	2
Laboratory Information .....	6
<b>FINDINGS AND RECOMMENDATIONS</b> .....	<b>7</b>
I. Compliance with NDIS Participation Requirements.....	7
Results of the OIG Audit .....	7
Conclusion .....	10
Recommendation .....	11
II. Compliance with Quality Assurance Standards .....	12
Results of the OIG Audit .....	12
Conclusion .....	17
Recommendation .....	17
III. Suitability of Forensic DNA Profiles in CODIS Databases .....	18
Results of the OIG Audit .....	19
Conclusion .....	23
<b>APPENDICES:</b>	
<b>I. OBJECTIVES, SCOPE, AND METHODOLOGY</b> .....	<b>24</b>
<b>II. AUDIT CRITERIA</b> .....	<b>27</b>
<b>III. AUDITEE RESPONSE</b> .....	<b>31</b>
<b>IV. DEPARTMENT OF JUSTICE RESPONSE</b> .....	<b>33</b>
<b>V. OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY     OF ACTIONS NECESSARY TO CLOSE THE REPORT</b> .....	<b>34</b>

# **AUDIT OF COMPLIANCE WITH STANDARDS GOVERNING COMBINED DNA INDEX SYSTEM ACTIVITIES AT THE SAN FRANCISCO POLICE DEPARTMENT CRIMINALISTICS LABORATORY SAN FRANCISCO, CALIFORNIA**

## **INTRODUCTION**

The Department of Justice Office of the Inspector General (OIG), Audit Division, has completed an audit of compliance with standards governing Combined DNA Index System (CODIS) activities at the San Francisco Police Department Criminalistics Laboratory, San Francisco, California (SFPD Laboratory).

### **Background**

The Federal Bureau of Investigation's (FBI) CODIS provides an investigative tool to federal, state, and local crime laboratories in the United States using forensic science and computer technology. 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 generally covered the period from January 2009 through December 2010. The objectives of our audit were to determine if the: (1) SFPD Laboratory was in compliance with the National DNA Index System (NDIS) participation requirements; (2) SFPD Laboratory was in compliance with the Quality Assurance Standards (QAS) issued by the FBI; and (3) SFPD Laboratory's forensic DNA profiles in CODIS databases were complete, accurate, and allowable for inclusion in NDIS. Appendix I contains a detailed description of our audit objectives, scope, and methodology; and Appendix II contains the criteria used to conduct the audit.

---

<sup>1</sup> DNA, or deoxyribonucleic acid, is genetic material found in almost all living cells that contains encoded information necessary for building and maintaining life. Approximately 99.9 percent of human DNA is the same for all people. The differences found in the remaining 0.1 percent allow scientists to develop a unique set of DNA identification characteristics (a DNA profile) for an individual by analyzing a specimen containing DNA.

## **Legal Foundation for CODIS**

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

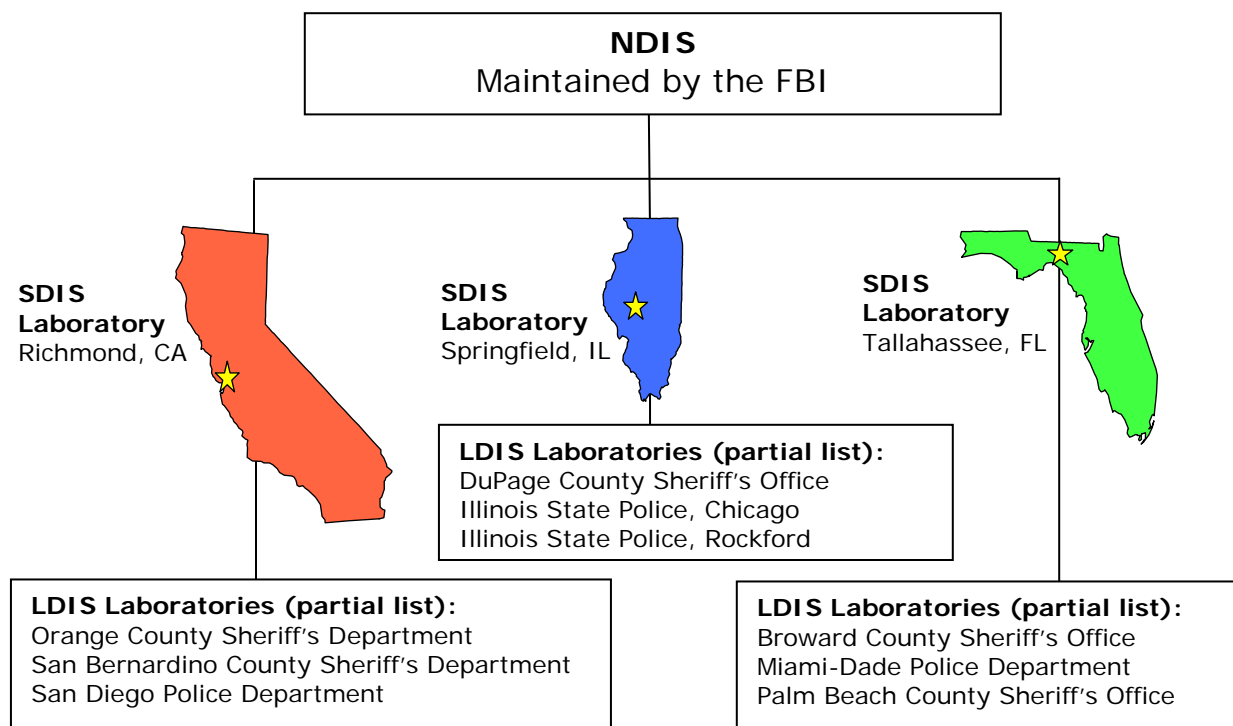
The FBI implemented CODIS as a distributed database with hierarchical levels that enables federal, state, and local crime laboratories to compare DNA profiles electronically. CODIS consists of a hierarchy of three distinct levels: (1) NDIS, managed by the FBI as the nation's DNA database containing DNA profiles uploaded by participating states; (2) the State DNA Index System (SDIS) which serves as a state's DNA database containing

---

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

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 Palm Beach County, Florida, Sheriff's Office sends its profiles to the state laboratory in Tallahassee, which then uploads the profiles to NDIS. Each state participating in CODIS has one designated SDIS laboratory. The SDIS laboratory maintains its own database and is responsible for overseeing NDIS issues for all CODIS-participating laboratories within the state. The graphic below illustrates how the system hierarchy works.

### Example of System Hierarchy within CODIS



### National DNA Index System

NDIS, the highest level in the CODIS hierarchy, enables laboratories participating in the CODIS program to electronically compare DNA profiles on a national level. NDIS does not contain names or other PII about the profiles. Therefore, matches are resolved through a system of laboratory-to-laboratory contacts. NDIS contains the following eight 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.<sup>4</sup>
- 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 for analysis and entry into NDIS.
- Forensic Index profiles originate from, and are associated with, evidence found at crime scenes.
- 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>5</sup>
- Relatives of Missing Person Index is comprised of DNA profiles generated from the biological relatives of individuals reported missing.

Given these multiple databases, 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

---

<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.

<sup>4</sup> An example of a Legal Index profile is one from a person found not guilty by reason of insanity who is required by the relevant state law to provide a DNA sample.

<sup>5</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.

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.

### *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 applicable state's SDIS 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. Although officials from LDIS laboratories do not sign an MOU, LDIS laboratories that upload DNA profiles to an SDIS laboratory are required to adhere to the MOU signed by the SDIS laboratory.

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.

CODIS becomes more useful as the quantity of DNA profiles in the system increases because the potential for additional leads rises. However, the utility of CODIS relies upon the completeness, accuracy, and quantity 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 DNA information that resulted from a DNA analysis and

may not be searched at NDIS.<sup>6</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 or an incorrect specimen number, may generate false positive leads, false negative comparisons, or lead to the misidentification of a 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 participation requirements and the profiles uploaded to CODIS are complete, accurate, and allowable for inclusion in NDIS.

## **Laboratory Information**

The SFPD Laboratory serves the City and County of San Francisco, California, which has a population of approximately 800,000. In addition, it provides services to the United States Park Police, which has law enforcement responsibilities within select areas of San Francisco.<sup>7</sup> The SFPD Laboratory participates in the CODIS program as an LDIS Laboratory. In 2000, the SFPD Laboratory began analyzing DNA as a means of processing evidence in criminal cases and in 2003 it began uploading forensic profiles into NDIS.

The SFPD Laboratory was first accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) in 2005 and was reaccredited in February 2010 for a period of 5 years. In August 2010, the SFPD Laboratory began utilizing the services of an outside laboratory, the Serological Research Institute, to analyze some of the SFPD Laboratory's DNA samples from less violent cases in order to reduce its backlog.

---

<sup>6</sup> A "locus" is a specific location on a chromosome. The plural form of locus is loci.

<sup>7</sup> The United States Park Police has law enforcement responsibilities in areas controlled by the U.S. Department of the Interior, National Park Services and that are located within the City and County of San Francisco. This includes the Golden Gate National Recreation Area and such areas as the Presidio, the Aquatic Park Historic District, Ocean Beach, and many other parks and monuments. The SFPD Laboratory estimates that it performs DNA analysis on 5 to 8 cases each year for the United States Park Police.

## **FINDINGS AND RECOMMENDATIONS**

### **I. Compliance with NDIS Participation Requirements**

The SFPD Laboratory was in compliance with NDIS participation requirements regarding updated training for Laboratory personnel, maintenance of training and qualification records for CODIS users, and timeliness of NDIS matches. We found that the SFPD Laboratory did not transfer back-ups of the CODIS server off-site on a monthly basis.

The NDIS participation requirements, which consist of the MOU and the NDIS Procedure Manual, establish the responsibilities and obligations of laboratories that participate in the CODIS program at the national level. The MOU describes the CODIS-related responsibilities of both the SFPD Laboratory and the FBI. The NDIS Procedure Manual is comprised of the NDIS operational procedures and provides detailed instructions for laboratories to follow when performing certain procedures pertinent to NDIS. The NDIS participation requirements we reviewed are included in Appendix II of this report.

#### **Results of the OIG Audit**

We found that the SFPD Laboratory did not comply with the NDIS participation requirements because it did not back up its CODIS server on a weekly basis and transport backed up CODIS data to an off-site location on a monthly basis. We describe this in more detail below.

##### *Server Back-Ups*

The NDIS Security Requirements state that laboratories participating in NDIS are responsible for backing up local CODIS data on at least a weekly basis. Further, the same laboratories must store CODIS back-up media at a secure, off-site location on at least a monthly basis. We found that the SFPD Laboratory did not back up its CODIS data in full accordance with NDIS requirements. The SFPD Laboratory's CODIS Administrator explained that since 2003, the SFPD Laboratory had been backing up its CODIS data and storing it at an off-site facility on a quarterly basis. SFPD Laboratory officials considered this process to be acceptable because the Laboratory was also uploading its forensic profiles to California's SDIS laboratory on a weekly basis and SFPD Laboratory officials regarded the weekly uploads as being similar to locally backing up its CODIS data.

The SFPD Laboratory deviated from the NDIS Security Requirements regarding its CODIS back-up procedures. First, information provided to us during our site work at the Laboratory indicated it was not backing up its CODIS data every week as required.<sup>8</sup> Second, it was not storing its CODIS database back-ups at an off-site location on a monthly basis as required. These deviations are a concern, especially based upon our observation that personnel that are not part of the DNA Analysis Unit were able to have physical access to the CODIS server. Further, SFPD's reliance on its weekly upload to the California SDIS laboratory cannot be considered proper data management practice because it shifts responsibility for properly backing up local CODIS data from the SFPD to another laboratory. We believe that these deficiencies pose a significant risk in that the SFPD Laboratory's CODIS server will not be reloaded with the most up-to-date data in the event of a natural disaster, accidental error, system crash, or any type of physical tampering or disturbance. Therefore, we recommend that the FBI work with the SFPD Laboratory to establish procedures that would ensure that the SFPD's CODIS server is backed up at least once a week and that back-ups are stored off-site on at least a monthly basis.

Besides this issue stated above, we had no other significant concerns related to the SFPD Laboratory's compliance with the other NDIS participation requirements we reviewed. The results of our audit are described in more detail below:

- The NDIS General Responsibilities Operational Procedures manual requires that participating laboratories ensure that CODIS users are notified of and provided access to revised NDIS Operational Procedures and other documentation necessary to properly participate in NDIS. The SFPD Laboratory's CODIS Administrator stated that the Laboratory provides its personnel with copies of the NDIS procedure manual, in addition to its availability on the FBI's Criminal Justice Information System—Wide Area Network. The SFPD Laboratory's CODIS Administrator stated that she also provides verbal guidance and informational updates to CODIS users at the SFPD Laboratory when needed. Finally, we selected two of the six CODIS users to interview and determined that both users understood NDIS procedures and could access the procedures if needed.

---

<sup>8</sup> The SFPD's response to our draft audit report stated that the SFPD Laboratory's procedures for backing up its CODIS server and related data included performing back-ups on a daily basis using a software program. We are working with the SFPD Laboratory and the FBI to confirm this information.

- The NDIS Security Requirements state that the CODIS server and equipment and hardware shall be electronically safeguarded from unauthorized use and be only accessible to a limited number of approved personnel. We found that only a limited number of CODIS users within the SFPD Laboratory have access to CODIS through the FBI's Criminal Justice Information System—Wide Area Network. This access is further limited to one computer workstation. We observed that all SFPD Laboratory CODIS users have their own CODIS accounts, unique passwords, and must undergo annual CODIS training. Moreover, the SFPD Laboratory's in-house policy limits access to the CODIS database to only the CODIS Administrator and her alternate. Other SFPD CODIS users utilize the single computer workstation that has access to CODIS in order to participate in annual online CODIS training.
- The NDIS Security Requirements state that only authorized personnel shall have physical access to the CODIS server, and that maintaining the server in a separate room of the laboratory or in another locked space or cabinet is not required provided access to the CODIS server is controlled in accordance with the requirements of this procedure. We learned that the CODIS server has been stored in a limited-entry unit of the SFPD Laboratory space since 2003. Access to this unit is currently limited to seven laboratory personnel and staff who hold supervisory positions within the Laboratory. We observed the location and accessibility of the CODIS server and found it to be in compliance with NDIS Security Requirements.
- SFPD Laboratory CODIS users are required to complete annual DNA Records Acceptance training. The FBI provided to us a list of SFPD Laboratory personnel who had received this mandatory annual training, which we compared to a list provided by the Laboratory. We found that all authorized personnel have successfully completed the annual training.
- 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 all six SFPD Laboratory CODIS users.
- At the time of our audit, the NDIS General Responsibilities Operational Procedures manual required participating laboratories to maintain records of CODIS users, including reports concerning

proficiency testing, and any other reports or audits required by the FBI, for a period of 10 years. We determined that SFPD Laboratory maintained personnel files for its CODIS users indefinitely, which is in accordance with its in-house policy requirement and in compliance with the 10-year retention requirement that was in the NDIS Operational Procedures.

- The NDIS Interstate Candidate Match Operational Procedures defines procedures for participating laboratories to follow when confirming matches that are identified in the CODIS system. We reviewed a sample of five NDIS matches and determined that each match was generally confirmed and, when applicable, investigators were notified in a timely manner. Specifically, we found:
  - The SFPD Laboratory sent confirmation requests in a timely manner for all five matches;
  - Confirmation generally took place within 30 days after the SFPD Laboratory's request was sent out for four of the five matches. For the one late match confirmation, the process took 66 days because another laboratory did not confirm the match submitted by the SFPD Laboratory in a timely manner;
  - The SFPD Laboratory notified investigators of match confirmation in a timely manner for all five matches.
- The NDIS operational procedure entitled *Review of External Audits* requires that an external quality assurance review be forwarded to the FBI's NDIS Custodian within 30 days of the participating laboratory's receipt of the report. We reviewed the submission of the most recent external review and found that the report was submitted to the FBI's NDIS Custodian in a timely manner.

## **Conclusion**

We found that the SFPD Laboratory did not store CODIS server back-ups at an off-site location, other than the NDIS Participating Laboratory, on a monthly basis.

## **Recommendation**

We recommend that the FBI:

1. Work with the SFPD Laboratory to establish procedures to ensure back-ups of its CODIS server are performed at least once a week and those back-ups are maintained at an off-site location at least on a monthly basis.



## II. Compliance with Quality Assurance Standards

We found that the SFPD Laboratory complied with the QAS issued by the FBI regarding the performance of QAS reviews within designated timeframes, and the proper monitoring of its subcontractors to ensure data integrity.<sup>9</sup> However, we also found that security at the SFPD Laboratory did not fully meet Forensic QAS that outline personnel access to the DNA Analysis Unit.

During our audit, we considered the Forensic QAS issued by the FBI.<sup>10</sup> These standards describe the quality assurance requirements that the SFPD Laboratory was required to adhere to in order to ensure its data met quality and integrity standards. We also assessed the two most recent QAS reviews that were conducted of the SFPD Laboratory. The QAS we reviewed are listed in Appendix II.

### Results of the OIG Audit

We noted one exception to the SFPD Laboratory's compliance with Forensic QAS. Specifically, we found that the SFPD Laboratory did not adhere to the Forensic QAS that requires access to the laboratory to be controlled and limited in a manner to prevent access by unauthorized personnel. The results of our audit are described in more detail below.

#### *Controlled and Limited Access to the Laboratory*

During our audit, we observed the SFPD Laboratory's security measures for limiting entry and access into its facility, and more specifically into its DNA Analysis Unit, to only include authorized personnel. We identified security measures, such as key locks and combination touch pads, which the SFPD Laboratory has in place to secure access to its building from the outside. The SFPD Laboratory staff members told us that the interior

---

<sup>9</sup> The QAS requires that laboratories undergo annual audits. Every other year, the QAS requires that the audit be performed by an external agency that performs DNA identification analysis and is independent of the laboratory being reviewed. These audits are not required by the QAS to be performed in accordance with the *Government Auditing Standards* (GAS) and are not performed by the Department of Justice Office of the Inspector General. Therefore, we will refer to the QAS audits as reviews (either an internal laboratory review or an external laboratory review, as applicable) to avoid confusion with our audits that are conducted in accordance with GAS.

<sup>10</sup> Forensic Quality Assurance Standards refer to the Quality Assurance Standards for Forensic DNA Testing Laboratories, effective July 1, 2009.

doors within the SFPD Laboratory leading into the DNA Analysis Unit were accessible to all laboratory personnel and were not limited to just the staff members that were assigned to the DNA Analysis Unit.

We observed that the door between the Firearms Unit and the DNA Analysis Unit was propped open, along with another open door from the Firearms Unit to an unlocked corridor within the SFPD Laboratory.<sup>11</sup> This corridor led to the front lobby of the building, to the garage that housed the San Francisco Police Department (SFPD) vehicle fleet, and one of the SFPD Laboratory's secure evidence areas. We observed Laboratory staff working in the Firearms and DNA Analysis Units while these doors were propped open. SFPD Laboratory management explained that the series of open doors was an infrequent occurrence and that the doors were kept open in an attempt to equalize the temperatures between the spaces occupied by the Firearms Unit and DNA Analysis Unit. However, we are concerned that visitors or personnel with limited access to the SFPD Laboratory's facilities or garage area could gain unauthorized access to the DNA Analysis Unit through propped open doors and the unlocked corridor. This vulnerability is compounded in those instances where there may not be SFPD Laboratory staff present to prevent unauthorized personnel from entering the secured DNA Analysis Unit.

Further, we learned that other SFPD units, not related to the SFPD Laboratory, periodically use space within the SFPD Laboratory for law enforcement training courses attended by non-Laboratory personnel. The SFPD Laboratory's Quality Assurance Manager did not feel these trainings were a security concern for the SFPD Laboratory and explained that the foot traffic within the Laboratory is monitored and that attendees are escorted upstairs and through other areas of the building. However, we believe that the presence of regular visitors in the facility increases the risk of unauthorized access to the DNA Analysis Unit, and thereby underscores the need to maintain adequate security of the Laboratory. We do not believe that SFPD Laboratory is in compliance with the Forensic QAS that states that

---

<sup>11</sup> According to the September 2010 ASCLD/LAB Interim Inspection Report, ASCLD/LAB inspectors visited the SFPD Laboratory in August 2010 to investigate concerns about the Laboratory, including allegations of possible unrestricted access that were raised in an anonymous letter. According to the report the SFPD Quality Assurance Manager stated that prior to November 2009 she observed doors to the building and Laboratory secure areas being propped open, but that this practice stopped after the SFPD Laboratory installed a proximity card access system. The September 2010 report concluded that the ASCLD/LAB inspectors did not observe any doors being propped open and that the SFPD Laboratory was meeting ASCLD/LAB's security requirements.

access should be controlled and limited in a manner to prevent access by unauthorized personnel. We recommend that the FBI work with the SFPD Laboratory to enhance security for the DNA Laboratory.

We found that the SFPD Laboratory complied with the other NDIS QAS that we reviewed, as described below:

- The QAS requires laboratories to undergo an annual review, including an external review every 2 years. As of January 2011, we found that the SFPD Laboratory had external QAS reviews performed in November 2009 and April 2010, and an internal QAS review in December 2010.
- We reviewed the prior 2 years of QAS review reports for the SFPD Laboratory. Both the internal and external reviews were conducted using the FBI's QAS Review Document. The FBI confirmed that at least one of the QAS reviewers for both reviews had successfully completed the FBI QAS Review training course.
  - The two external reviews we examined identified four findings, two of which were overturned by the NDIS Audit Review Panel. The remaining two findings reported that: (1) the SFPD Laboratory failed to provide its preceding review report to the FBI within the required 30 days; and (2) the SFPD Laboratory uploaded different alleles than those listed by the DNA analyst on the CODIS upload form without concurrence of the DNA analyst. We reviewed the SFPD Laboratory's corrective actions and determined that it had taken appropriate action to remedy these errors including the establishment of a new policy within its DNA Quality Assurance Manual to provide external audit documentation and laboratory responses to the FBI within 30 days of receiving the audit documentation or report. In addition, the SFPD Laboratory clarified its procedure to verify criteria for DNA profiles through two concordant assessments that are to be prepared by qualified analysts or technical reviewers.
  - The internal QAS review did not identify any findings of non-compliance.
- We asked each of the QAS reviewers who conducted the most recent external QAS reviews to certify that they had no impairments to independence. All QAS reviewers provided us with this certification.

- We reviewed the SFPD Laboratory's policies on physical security of the facility as well as the access key card assignments for the secured areas of the Laboratory. We also toured the SFPD Laboratory and observed that the facility remains locked and closed to the public at all times; authorized SFPD Laboratory personnel enter using a key or numerical touch pad. We observed that the facility is protected during after-hours by motion detectors and an alarm system. While we noted internal security concerns pertaining to the DNA Analysis Unit that are mentioned above, we found that overall external security at the SFPD Laboratory is adequate and in compliance with the QAS requirements we tested.
- The QAS requires laboratories to perform evidence examination, DNA extraction, and polymerase chain reaction (PCR) setup processes at separate times or in separated spaces. We reviewed the policies and procedures that the SFPD Laboratory implements regarding the separation of known and unknown DNA samples in accordance with the QAS requirements. According to the SFPD Laboratory's Quality Control Manual standard, evidence samples should be separated by time or space. We did not identify any material deficiencies with regard to the SFPD Laboratory's separation of known and unknown DNA samples, which are processed at separate times.
- The integrity of physical evidence is maintained by the Laboratory in accordance with the QAS requirements that we tested. Sample evidence is placed in containers that are labeled with the SFPD Laboratory's incident number and the SFPD Property Record Item number. Each DNA Analyst who takes custody of the evidence will mark the outer container with their initials and date. Specifically, we reviewed the SFPD Laboratory's policy for retaining samples and found that the SFPD Laboratory retains sample extracts indefinitely and stores these sample extracts in the DNA Analysis Unit. In the DNA Analysis Unit, we observed that sample extracts are maintained in refrigerators unlocked during business hours and locked after-hours. SFPD Laboratory officials confirmed this practice. The extracts and evidence samples are formally transferred from the DNA Analysis Unit and held long-term in the SFPD's Property Control Division. We viewed evidence of transfer paperwork and Property Control Division evidence control and release policies and determined that they were clear, detailed, and adequate to ensure evidence is properly handled and transferred to the Property Control Division.

- We found that since July 2010, the SFPD Laboratory has contracted with a vendor laboratory, Serological Research Institute, to outsource some of its forensic analysis work. We reviewed the Serological Research Institute's most recent accreditation obtained in December 2009, its QAS audit documentation from September 2009, and the contract that the SFPD Laboratory holds with the Serological Research Institute. Between July 2010 and April 2011, the SFPD Laboratory outsourced approximately 250 cases.<sup>12</sup> During our site visit, we learned that in December 2010, the SFPD Laboratory had temporarily stopped outsourcing samples to the Serological Research Institute because of possible contamination issues identified by the SFPD Laboratory. However, after reviewing the results from a contamination study completed in January 2011 the Laboratory has since resumed outsourcing casework to the Serological Research Institute.
- We reviewed the SFPD Laboratory's procedures for verifying vendor casework and found that a technical review is performed and documented for all outsourced samples eligible for upload into CODIS. The SFPD Laboratory's technical review procedure for vendor casework is identical to that of in-house casework and is in accordance with the QAS requirements.<sup>13</sup> As of March 2011, all cases outsourced to the Serological Research Institute that were deemed eligible for CODIS upload by the vendor laboratory had successfully passed the SFPD Laboratory's technical review process.
- We reviewed the documentation of SFPD Laboratory's site visit to Serological Research Institute and verified that the Laboratory conducted a site visit of the facility in July 2010, prior to entering into a contract with the Serological Research Institute. During that site visit, the SFPD Laboratory found no issues with the Serological Research Institute's operations.

---

<sup>12</sup> As of April 2011, the SFPD had uploaded 21 outsourced cases into NDIS.

<sup>13</sup> FBI QAS 17.5.1 states that technical review shall include the following elements: (1) a review of all DNA types to verify that they are supported by the raw or analyzed data (electropherograms or images); (2) a review of all associated controls, internal lane standards, and allelic ladders to verify that the expected results were obtained; (3) a review of the final report (if provided by vendor laboratory) to verify that the results and conclusions are supported by the data; and (4) verification of the DNA types, eligibility, and the correct specimen category for entry into CODIS.

## **Conclusion**

We found that the SFPD Laboratory complied with the FBI's Forensic QAS that we tested, with one exception. During our visit to the Laboratory, we observed multiple sets of doors propped open that led from the main lobby, through an unlocked corridor, and ultimately to the DNA Analysis Unit. Based on this observation, the SFPD Laboratory did not fully comply with FBI's Forensic QAS that requires access to the laboratory to be controlled and limited. Although the SFPD Laboratory has a policy in place regarding physical security controls for limiting unauthorized access into the unit, the SFPD Laboratory needs to strengthen its adherence to that policy and ensure it is consistently followed by all staff so that access to the DNA Analysis Unit remains secure and limited to SFPD Laboratory personnel who are authorized to have access to that unit.

## **Recommendation**

We recommend that the FBI:

2. Work with the SFPD Laboratory to enhance its security procedures for preventing access to the DNA Laboratory by unauthorized personnel.

### III. Suitability of Forensic DNA Profiles in CODIS Databases

We found that 7 of the 100 profiles we reviewed did not meet NDIS or SFPD Laboratory's suitability standards. The SFPD Laboratory removed all seven profiles from NDIS. Specifically, we found: (1) two profiles violated the 4x4 rule; (2) three profiles were obtained from the suspect's person or residence, (3) one profile was developed from evidence not connected to a crime; and (4) one profile did not meet the SFPD Laboratory's own minimum requirement of seven core loci for uploading to CODIS.<sup>14</sup>

We reviewed a sample of the SFPD Laboratory's forensic DNA profiles to determine whether each profile was complete, accurate, and allowable for inclusion in NDIS.<sup>15</sup> To test the completeness and accuracy of each profile, we established standards that require a profile include all the loci for which the analyst obtained results, and that the values at each locus match those identified during analysis.<sup>16</sup> Our standards are described in more detail in Appendix II of this report.

The FBI's NDIS operational procedures establish the DNA data acceptance standards by which laboratories must abide. The FBI also developed a flowchart as 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

---

<sup>14</sup> The "4x4 rule", published by the FBI in September 2003, is a reference to Section 6.4.6 of the NDIS DNA Data Acceptance Standards, which states that forensic mixture DNA profiles submitted to NDIS may have up to 4 alleles at a maximum of 4 core loci, provided that the remaining 9 core loci have no more than 2 alleles at each locus.

<sup>15</sup> When a laboratory's universe of DNA profiles in NDIS exceeds 1,500, our sample is taken from SDIS rather than directly from NDIS. See Appendix I for further description of the sample selection.

<sup>16</sup> A "locus" is a specific location on a chromosome. The plural form of locus is loci.

generally not a forensic unknown and would not be allowable for upload to NDIS. The NDIS procedures we reviewed are listed in Appendix II of this report.

## **Results of the OIG Audit**

We selected a sample of 100 profiles out of the 935 forensic profiles that the SFPD Laboratory had uploaded into NDIS as of December 22, 2010. Of the 100 forensic profiles sampled, we found that 7 profiles were unallowable for upload to NDIS. The remaining profiles sampled were complete, accurate, and allowable for inclusion in NDIS. The specific exceptions are explained in more detail below.

### *Profile Allowability*

Based on our review, we found 7 of the 100 profiles in our sample did not meet NDIS requirements and were unallowable for upload into the NDIS database. The remaining 93 profiles were complete, accurate, and allowable for NDIS upload. Our review examined each profile in the sample to determine its suitability based on NDIS guidelines such as: (1) whether a crime was committed; (2) whether the profile was obtained from the crime scene; and (3) whether the profile was attributable to a putative perpetrator.

Specifically, we identified the following seven profiles not suitable for CODIS: (1) two profiles were not allowable for upload because they violated the 4x4 rule; (2) three profiles were not allowable because they were obtained from the suspect's person or residence; (3) one profile was obtained from an item that was not connected to a crime; and (4) one profile did not meet the Laboratory's minimum requirement of seven core loci for upload to CODIS. The results of our review are further explained below:

### *OIG Sample Number CA-20*

Sample CA-20 was taken from the suspect's clothing. This clothing was retrieved from the suspect 1 week after the homicide was committed. We deemed this profile to be unallowable because it is considered a deduced suspect profile rather than a forensic unknown profile, and it was not



retrieved from the crime scene.<sup>17</sup> We presented this to the SFPD Laboratory CODIS Administrator, who agreed that this profile was unallowable and removed it from CODIS.

*OIG Sample Number CA-37*

Sample CA-37 was taken from a swab of a gun grip retrieved during a police chase of the suspects. There were six core loci uploaded into CODIS because according to the case file documentation, alleles at three core loci could not be detected. We presented this to the CODIS Administrator, who stated that there was not enough DNA to test 13 core loci. The SFPD Laboratory's requirement is to test the profile on at least nine core loci and upload a minimum of seven to SDIS; therefore, the SFPD Laboratory did not adhere to its own minimum loci requirement when it uploaded this case. The CODIS Administrator determined that the profile was not suitable and removed it from CODIS.

*OIG Sample Number CA-44*

Sample CA-44 was taken from a cigarette butt found in a trash can in connection with a death investigation. However, the information in the case file was not sufficient to connect the cigarette butt to a putative perpetrator. In addition, as of January 2011, the cause of the victim's death was listed as undetermined and could not definitively be ruled as a homicide, even though the case file stated there were suspicious circumstances surrounding the victim's death. As a result, we determined that this profile was unallowable. We presented this to the CODIS Administrator who agreed with our determinations and removed the profile from CODIS.

*OIG Sample Number CA-45*

Sample CA-45 was taken from a stain on bedding in a room where a rape had occurred. The victim was raped by five males at the apartment where several of the suspects resided. We deemed this profile to be unallowable because the suspects of the crime also resided at the apartment, and we could not be sure that this particular forensic mixture was attributed to the crime. We reviewed the DNA analysis results for the non-sperm fraction of the mixture and found that it did not match the victim's standard; therefore, it appeared that this stain may have come from an unrelated sexual act that did not involve the victim. We presented this to

---

<sup>17</sup> FBI introduced guidance to exclude deduced suspect profiles from NDIS in 2006. To be classified as a forensic unknown record, the DNA sample must be attributed to the putative perpetrator. Items taken directly from the suspect are considered deduced suspect samples, not forensic unknowns, and are not eligible for upload to NDIS.

the CODIS Administrator, who agreed that this profile was unallowable and removed it from CODIS.

#### *OIG Sample Number CA-50*

Sample CA-50 was taken from a condom found in the male victim's apartment where a rape occurred. We determined that the sample was unallowable because it violated the FBI's 4x4 rule and was uploaded to CODIS in February 2005, after the 4x4 rule was established. The profile presented three alleles at six loci and two alleles at each of the remaining three loci. We presented this to the CODIS Administrator, who agreed that the profile was unallowable and removed it from CODIS.

#### *OIG Sample Number CA-74*

We determined that sample CA-74 was unallowable because it violated the FBI's 4x4 rule and was uploaded to CODIS in September 2004, after the 4x4 rule was established. The profile was a mixture of two suspects and presented four alleles at four core loci and three alleles at each of the remaining six core loci. We presented this to the CODIS Administrator, who agreed that the profile was unallowable and removed it from CODIS.

#### *OIG Sample Number CA-96*

Sample CA-96 was taken from a genital swab of the suspect. We deemed this profile to be unallowable because it is not a forensic unknown profile, but rather a deduced suspect profile. We presented this to the CODIS Administrator, who agreed that the profile was unallowable and removed it from CODIS.

#### *Other Matters*

As a result of our audit, we found that the SFPD Laboratory does not always attempt to obtain results for all 13 core loci. Specifically, for 55 of the 100 profiles we reviewed, the Laboratory analyzed the profile using the Profiler Plus<sup>®</sup> PCR Amplification Kit, which produces results for only 9 of the 13 core loci.<sup>18</sup> NDIS guidelines for CODIS index search parameters set the minimum number of loci required to report a match at 10 core loci, which essentially precludes profiles with less than 10 core loci from being searched at NDIS and providing investigative leads to other states.

---

<sup>18</sup> Of the 55 total profiles that were analyzed on Profiler Plus and produced results at 9 core loci, we determined 6 profiles to be unallowable during the course of our review.

When we inquired about this issue, the CODIS Administrator stated that the Profiler Plus<sup>®</sup> PCR Amplification Kit was attempted only when one of the following situations arose:

1. there was insufficient DNA to conduct the testing on all 13 core loci;
2. analysis was performed prior to December 2002 when the SFPD Laboratory validated the COfiler<sup>®</sup> PCR Amplification kit, which provides results for the remaining 4 core loci;
3. the DNA analyst was presented by the investigator with a potential match for the forensic profile to a suspect; or
4. the case was determined to be solved.

We agree with the SFPD Laboratory that COfiler<sup>®</sup> could not be utilized before it was validated or if there was insufficient DNA to test on all 13 loci. However, we do not believe that the SFPD Laboratory's last two reasons listed above should preclude profiles from being searched at NDIS. We determined that 19 of the 55 profiles could have been tested on all 13 core loci because the DNA analysis took place after December 2002, when COfiler<sup>®</sup> was instituted at the SFPD Laboratory, and there was sufficient DNA to test on 13 core loci.<sup>19</sup>

Our concern is that by purposefully analyzing and uploading to NDIS forensic profiles that were analyzed on only 9 core loci when there was the possibility to analyze profiles on 13 core loci, the SFPD Laboratory was precluding other laboratories in other states from being able to search SFPD Laboratory's forensic profiles for possible matches. Therefore, we believe that the SFPD Laboratory was not fully participating in NDIS, as it was not fully adhering to the NDIS DNA Data Acceptance Standards, which require that analysis on all 13 core loci be attempted for forensic unknown profiles. We asked the CODIS Administrator about this issue and she stated that 2 years ago, the SFPD Laboratory had begun efforts to perform additional testing on samples that had only been tested on 9 core loci using Profiler Plus. However, 2 months after the effort began, the Criminalist assigned to this project resigned and the project was stalled. The CODIS Administrator stated that this project will be restarted and the SFPD Laboratory plans to conduct testing using COfiler<sup>®</sup> for those samples that had previously been analyzed only on nine core loci in order to obtain results for the additional

---

<sup>19</sup> This total of 19 profiles does not include the 6 profiles that we determined to be unallowable during the course of our review.

four core loci and upload complete profiles into NDIS. As of July 2011, the CODIS Administrator could not provide a definite date for when the project will be restarted, but instead gave an estimated timeframe of 6 to 12 months from July 2011, which includes the time it will take to acquire and train new personnel.

## **Conclusion**

Based on our testing of 100 sample forensic profiles that the SFPD Laboratory uploaded to NDIS, we found 93 profiles were complete, accurate, and allowable for inclusion in NDIS. However, we also identified seven forensic profiles that were not suitable for upload to NDIS. The SFPD Laboratory took corrective action on all seven profiles and removed them from NDIS. We make no recommendations concerning the suitability of SFPD Laboratory's forensic DNA profiles that are in CODIS.

## APPENDIX I

### 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 2009 through December 2010. The objectives of the audit were to determine if the: (1) SFPD Laboratory was in compliance with the NDIS participation requirements; (2) SFPD Laboratory was in compliance with the QAS issued by the FBI; and (3) SFPD 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 SFPD Laboratory QAS review reports and supporting documentation for corrective action taken, if any, to determine whether: (a) the SFPD Laboratory complied with the QAS, (b) repeat findings were identified, and (c) recommendations were adequately resolved.<sup>20</sup>

In accordance with the QAS, the internal and external laboratory review procedures are to address, at a minimum, a laboratory's quality assurance program, organization and management, personnel qualifications, facilities, evidence control, validation of methods and procedures, analytical procedures, calibration and maintenance of instruments and equipment, proficiency testing of analysts, corrective action for discrepancies and errors, review of case files, reports, safety, and previous audits. 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.

---

<sup>20</sup> The QAS requires that laboratories undergo annual audits, which every other year must be performed by an external agency that performs DNA identification analysis and is independent of the laboratory being reviewed. The QAS does not require these audits to be performed in accordance with the *Government Auditing Standards* (GAS) and they are not performed by the Department of Justice Office of the Inspector General. Therefore, we refer to the QAS audits as either internal or external laboratory reviews, as applicable, to avoid confusion with our audits that are conducted in accordance with GAS.

As permitted by GAS 7.42 (2007 revision), we generally relied on the results of the SFPD Laboratory's external laboratory review to determine if the SFPD Laboratory complied with the QAS.<sup>21</sup> In order to rely on the work of non-auditors, GAS requires that we perform procedures to obtain sufficient evidence that the work can be relied upon. Therefore, we: (1) obtained evidence concerning the qualifications and independence of the individuals who conducted the review and (2) determined that the scope, quality, and timing of the audit work performed was adequate for reliance in the context of the current audit objectives by reviewing the evaluation procedure guide and resultant findings to understand the methods and significant assumptions used by the individuals conducting the reviews. Based on this work, we determined that we could rely on the results of the SFPD Laboratory's external laboratory review.

- Interviewed SFPD Laboratory officials to identify management controls, SFPD Laboratory operational policies and procedures, SFPD Laboratory certifications or accreditations, and analytical information related to DNA profiles.
- Toured the SFPD 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 SFPD Laboratory's written policies and procedures related to conducting internal reviews, resolving review findings, expunging DNA profiles from NDIS, and resolving matches among DNA profiles in NDIS.
- Reviewed supporting documentation for five matches to determine whether they were resolved in a timely manner. The SFPD Laboratory provided the universe of 23 matches as of January 10, 2011. The sample was judgmentally selected to include both case-to-case and case-to-offender matches. This non-statistical sample does not allow projection of the test results to all matches.

---

<sup>21</sup> We also considered the results of the SFPD Laboratory's internal laboratory review, but could not rely on it because it was not performed by personnel independent of the SFPD Laboratory. Further, as noted in Appendix II, we performed audit testing to verify SFPD Laboratory's compliance with specific QAS that have a substantial effect on the integrity of the DNA profiles uploaded to NDIS.

- Reviewed supporting documentation to determine whether the SFPD 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.

Working in conjunction with the contractor used by the FBI to maintain NDIS and the CODIS software, we obtained an electronic file identifying the 935 STR forensic profiles the SFPD Laboratory had uploaded to NDIS as of December 22, 2010. 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 randomly selected a representative sample of labels associated with specific profiles in our universe to reduce the effect of any patterns in the list of profiles provided to us. 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 SFPD 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 II for detailed information on our audit criteria.

After we issued our draft report to the FBI and the SFPD Laboratory, we learned from local news reports that the SFPD had recently conducted an internal investigation of its CODIS Administrator. In addition, the same local media reports also stated that the San Francisco District Attorney's Office had provided in writing to the SFPD its concerns related to the SFPD's DNA Laboratory. The SFPD did not inform us of these two matters during our fieldwork. Therefore, upon learning of these issues, we requested that the SFPD provide the following for our review: (1) the results of its internal investigation pertaining to its CODIS Administrator, and (2) the San Francisco District Attorney's Office written concerns with the SFPD's DNA Laboratory. Based on our review of these matters, we made no changes to the findings in our audit report.

## APPENDIX II

### AUDIT CRITERIA

In conducting our audit, we considered the NDIS participation requirements and the QAS. However, we did not test for compliance with elements that were not applicable to the SFPD 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 participation requirements, which consist of the Memorandum of Understanding (MOU) and the NDIS operational procedures, establish the responsibilities and obligations of laboratories that participate in NDIS. The MOU requires that NDIS participants comply with federal legislation and the QAS, as well as NDIS-specific requirements accompanying the MOU in the form of appendices. We focused our audit on specific sections of the following NDIS requirements.

- DNA Data Acceptance Standards
- DNA Data Accepted at NDIS
- QAS Reviews
- NDIS DNA Autosearches
- Confirm an Interstate Candidate Match
- General Responsibilities
- Initiate and Maintain a Laboratory's Participation in NDIS
- Security Requirements
- CODIS Users
- CODIS Administrator Responsibilities
- Access to, and Disclosure of, DNA Records and Samples
- Upload of DNA Records
- Expunge a DNA Record
- The FBI Flowchart: A Guide to Determining What is Allowable in the Forensic Index at NDIS<sup>22</sup>

---

<sup>22</sup> The FBI Flowchart is guidance issued to NDIS-participating laboratories separate from the MOU and NDIS operational procedures. The flowchart is contained in the 2010 CODIS Administrator's Handbook and has been provided to laboratories in referendums such as CODIS conferences.



## Quality Assurance Standards

The FBI issued two sets of QAS: QAS for Forensic DNA Testing Laboratories, effective July 1, 2009, (Forensic QAS); and QAS for DNA Databasing Laboratories, effective July 1, 2009, (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 generally relied on the reported results of the Laboratory's most recent annual external review to determine if the Laboratory was in compliance with the QAS. Additionally, we 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): 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): The laboratory shall have and follow a documented sample inventory control system to ensure the integrity of database and known samples.
- 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 audit shall be conducted by an audit team comprised of qualified auditors from a second agency(ies) and having at least one team member who is or has been previously qualified in the laboratory's current DNA technologies and platform.
- Outsourcing (Forensic QAS 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 results. Our rationale for this standard is that the probability of a false match among DNA profiles is reduced as the number of loci included in a profile increases. A false match would require the unnecessary use of laboratory resources to refute the match.
- **Accuracy of DNA Profiles:** The values at each locus of a profile must match those identified during analysis. Our rationale for this

standard is that inaccurate profiles may: (1) preclude DNA profiles from being matched and, therefore, the potential to link convicted offenders to a crime or to link previously unrelated crimes to each other may be lost; or (2) result in a false match that would require the unnecessary use of laboratory resources to refute the match.

- Timely Notification of Law Enforcement When DNA Profile Matches Occur in NDIS: Laboratories should notify law enforcement personnel of NDIS matches within 2 weeks of the match confirmation date, unless there are extenuating circumstances. Our rationale for this standard is that untimely notification of law enforcement personnel may result in the suspected perpetrator committing additional, and possibly more egregious, crimes if the individual is not deceased or already incarcerated for the commission of other crimes.

## AUDITEE RESPONSE

21 SEP 2011



EDWIN M. LEE  
MAYOR

POLICE DEPARTMENT  
CITY AND COUNTY OF SAN FRANCISCO  
THOMAS J. CAHILL HALL OF JUSTICE  
850 BRYANT STREET  
SAN FRANCISCO, CALIFORNIA 94103-4003



GREGORY P. SUHR  
CHIEF OF POLICE

September 16, 2011

David J. Gaschke  
Regional Audit Manager  
San Francisco Regional Audit Office  
Office of the Inspector General  
U.S. Department of Justice  
1200 Bayhill Drive, Suite 201  
San Bruno, CA 94066

Dear Mr. Gaschke,

The Office of the Inspector General has provided a draft copy of their report related to their audit of the Crime Lab's DNA Unit for compliance with the CODIS system. The report identified two recommendations.

The first recommendation is related to CODIS data back-up procedures conducted by the Crime Lab. The auditors state *"We found that the SFPD Laboratory did not perform back-ups of its CODIS server on a weekly basis and did not store the back-ups at an off-site location, other than the NDIS participating Laboratory, on a monthly basis."* The NDIS procedures states that the NDIS participating laboratory shall be responsible for conducting backups of their CODIS data on a routine schedule but in no event, less than once per week. The SFPD Forensic Biology Unit uses a software program called Symantec Backup Exec version 12, to back-up the CODIS server and associated data on a daily basis; the back-up occurs every evening at 11pm.

The NDIS procedures states that on a routine basis, but in no event, less than once per month, the CODIS back-up media shall be stored at a secure physical location other than the NDIS Participating Laboratory. The SFPD Forensic Biology Unit uses an 800 GB, HP LT03 Ultrium RW data cartridge to back-up data, and this cartridge is stored at a secure physical location other than the Laboratory at the San Francisco Police Department headquarters located at 850 Bryant Street; however, we change data cartridges on a quarterly basis instead of monthly. All DNA profiles uploaded to CODIS at the local level are permanently stored at the State level. The CODIS administrator will ensure data cartridges are stored at the secure, off-site location, on a monthly basis.

The second recommendation was related to Crime Lab security measures. The auditors state, *"Specifically, we found that the SFPD Laboratory did not adhere to the Forensic QAS that requires access to the laboratory to be controlled and limited in a manner to*

*prevent access by unauthorized personnel.* " During the audit, the HVAC system experienced a malfunction in the Firearms Unit which resulted in an inordinate and constant supply of hot air channeled into the office space. In order to safeguard instrumentation and evidence that may have been damaged by the extreme temperature, unit supervisor John Sanchez opened the unit's two internal doors to allow the heat to vent out. This also alleviated the intolerable conditions for unit members allowing work to continue. Sanchez contacted the building engineer who responded and repaired the malfunctioning equipment.

During this event, all members of the Firearms Unit were present and conducting case work. The group included two sworn members of the SFPD. Sanchez and the members of the Firearms Unit remained in the unit for the duration of this incident. Security of the Firearms and DNA Units was never compromised or breached. All interior and exterior entrance/exit points remained operational and protected by security measures. No other individuals, other than those identified here, entered the unit.

Secondly, the OIG auditors expressed concern regarding access to the training room located on the second floor of Building 606. The Crime Lab Manager reviews all law enforcement requests for the use of the training room. Although the room is outside both administrative and lab space of the Crime Lab, the Crime Lab Manager has informed all training coordinators of the Crime Lab's security policy. The Crime Lab Manager advises all Crime Lab personnel in advance of scheduled training events. The Crime Lab Manager meets with all presenters and conducts additional security inspections on the dates of such events to ensure adherence to Crime Lab security measures. Although attendees are sworn law enforcement officers, their access to Crime Lab administrative or lab space is prevented by security inspections, electronic key card devices and combination locks.

The San Francisco Police Department Crime Lab will work with the FBI based their review.

Sincerely,



---

Lt. Daniel Perea  
Crime Lab Manager  
San Francisco Police Department Crime Laboratory

DEPARTMENT OF JUSTICE RESPONSE



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

September 26, 2011

David J. Gaschke  
Regional Audit Manager  
San Francisco Regional Audit Office  
Office of the Inspector General  
1200 Bayhill Drive, Suite 201  
San Bruno, CA 94066

Dear Mr. Gaschke:

Your memorandum to Director Mueller forwarding the draft report of the audit conducted at the San Francisco Police Department Crime Laboratory, San Francisco, California (Laboratory) has been referred to me for response.

Your draft report contained two recommendations relating to the Laboratory's compliance with the FBI's Memorandum of Understanding and *Quality Assurance Standards for DNA Testing Laboratories*. The CODIS Unit has reviewed your draft report and offers the following comments.

With respect to recommendation one relating to routine performance and maintenance of CODIS server back-ups, the Laboratory utilizes a software program to back-up its CODIS server daily and those back-up data cartridges are now stored at a secure, off-site location monthly. The CODIS Unit is satisfied that the Laboratory is securely storing its server back-ups more routinely. The CODIS Unit supports closure of this recommendation.

With respect to recommendation two relating to unauthorized access, the FBI has recommended that the Laboratory post a sign on the internal doors to the DNA laboratory indicating that they must remain closed and not propped open. The Laboratory is considering the FBI's recommendation.

Thank you for sharing the draft audit report with us. If you have any questions, please feel free to contact Jennifer C. Luttman, Chief of the CODIS Unit, at (703) 632-8315.

Sincerely,

Alice R. Isenberg, Ph.D  
Section Chief  
Biometrics Analysis Section  
FBI Laboratory

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

The OIG provided a draft of this audit report to the SFPD Laboratory and the FBI. Individual responses from the SFPD Laboratory and the FBI are incorporated in Appendices III and IV, respectively. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

**Recommendation Number:**

- 1. Resolved.** In its response to our draft audit report, the SFPD Laboratory stated that its Forensic Biology Unit backs up its CODIS server and associated data on a daily basis using a software program, called Symantec Backup. This procedure and the SFPD Laboratory's use of a back-up software was not communicated to us during our audit fieldwork or at our exit conference. During our audit, the CODIS Administrator stated that the SFPD Laboratory was uploading its forensic profiles to California's SDIS laboratory on a weekly basis and SFPD Laboratory officials regarded these weekly uploads as being similar to the SFPD Laboratory locally backing up its CODIS data. As we stated in our report, the Laboratory's weekly uploads to California's SDIS Laboratory do not constitute the required weekly local back-ups of the SFPD Laboratory's CODIS server. After we obtained the SFPD's response to our report, we contacted the SFPD Laboratory to determine whether the daily back-up procedures were new or whether they were in place during our audit. We were told by the CODIS Administrator that the daily back-ups and use of a software program were in place during our audit. We added clarifications to our report to acknowledge the SFPD Laboratory's new statements pertaining to its back-up procedures.

In addition, the SFPD Laboratory's response stated that its Forensic Biology Unit physically backs up data to cartridges and stores those cartridges at an alternate secure physical location. The SFPD Laboratory acknowledged that it was moving these data cartridges to an offsite secure location on a quarterly basis instead of on a monthly basis, as required by FBI policy. However, the SFPD Laboratory stated in its response that the CODIS Administrator will ensure data cartridges are stored at a secure, offsite location on a monthly basis, which is more frequent than its quarterly schedule that we identified during our audit.

The FBI stated that its CODIS Unit is satisfied that the SFPD Laboratory is securely storing its server back-ups on a more routine basis as indicated in the SFPD Laboratory's response, and it supports closure of this recommendation. This recommendation can be closed when the SFPD Laboratory provides us with evidence that it has formally adopted its daily and monthly CODIS server back-up procedures as written policy.

2. **Resolved.** In its response to our draft audit report, the SFPD Laboratory provided additional details of the circumstances that caused multiple doors to be propped open during our tour of the SFPD Laboratory. Specifically, the SFPD Laboratory's HVAC system experienced a malfunction that resulted in an excessive supply of hot air that needed to be dissipated. The SFPD Laboratory's Firearms Unit Supervisor elected to open the two internal doors to disperse the heat and stabilize the temperature for staff members that were working in the Unit. Also, the building engineer was called to repair the malfunctioning equipment. The SFPD Laboratory added that during this event, all interior and exterior points of entry and exit were protected by security measures, the Firearms Unit staff was present and conducting casework in the area, and that security of the Firearms and DNA Analysis Units were not compromised. As stated in our report, SFPD Laboratory management explained to us when we were on-site that the series of propped open doors was an infrequent occurrence.

Although we understand that the SFPD Laboratory had experienced a temperature issue, we continue to have concerns related to the security vulnerabilities caused by multiple doors being propped open because this appears to have been an issue in the past. According to the September 2010 ASCLD/LAB Interim Inspection Report, the SFPD Quality Assurance Manager stated that she had observed propped open doors to the building and laboratory prior to November 2009 when the Laboratory's proximity card access system was installed.<sup>23</sup> The ASCLD/LAB inspectors did not observe propped doors and stated in the September 2010 report that the Laboratory was meeting the security requirements of ASCLD/LAB. However, due to vulnerabilities associated with propped doors, even if it occurs on an infrequent basis, and in

---

<sup>23</sup> According to the September 2010 ASCLD/LAB Interim Inspection Report, ASCLD/LAB inspectors visited the SFPD Laboratory in August 2010 to investigate concerns about the Laboratory, including allegations of possible unrestricted access that were raised in an anonymous letter.

ASCLD/LAB, *Interim Inspection Report San Francisco Police Department Criminalistics Laboratory* (September 2010), 1-3.



consideration of these prior issues, we believe it is appropriate for the SFPD Laboratory to remedy the security issue found during our review.

The SFPD Laboratory also provided a response to our concern of possible unauthorized access by individuals visiting the training room located on the second floor of its facility. The SFPD Laboratory stated that the Crime Laboratory Manager reviews all law enforcement requests for the use of the training room and informs all training coordinators of the Laboratory's security policy. The SFPD Laboratory Manager advises all SFPD Laboratory personnel of upcoming training events, meets with training facilitators in advance of scheduled training events, and conducts additional security inspections on the dates of such events to ensure adherence to security policies and procedures. The SFPD Laboratory clarified that attendees are sworn law enforcement officers, but their access to the SFPD Laboratory's administrative or laboratory space is prevented by security inspections, electronic key card devices, and combination locks. We recognize that the SFPD Laboratory has a protocol in place to address security matters that may arise when training courses are held, and we do not feel that trainees' access to the training room on the second floor is an issue. Rather, we are concerned that given our observation of propped open doors to the SFPD Laboratory's DNA Analysis Unit, there is a potential for persons not affiliated with the Laboratory to enter this space when no Laboratory personnel are present to prevent unauthorized access.

The FBI suggested in its response that the SFPD Laboratory post a sign on the internal doors to its DNA Analysis Unit indicating that they must remain closed and not be propped open. This recommendation can be closed when the SFPD Laboratory provides evidence that it has enhanced security measures against unauthorized access to its DNA Analysis Unit.