Oakland Police Department Criminalistics Laboratory

DNA Instrumentation and Analysis Software

Biometric Technology Use Policy

June 2023

1. Purpose

The Oakland Police Department (OPD) Criminalistics Laboratory's (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to perform forensic DNA testing. During this lengthy and complicated process, one step removes and purifies DNA from cells (digestion/extraction), another quantitates how much DNA is present and lastly, by amplifying and analyzing Short Tandem Repeats (STR) in the DNA using Polymerase Chain Reaction (PCR) and separated by Capillary Electrophoresis (CE), forensic DNA profiles are generated. Software is involved in the following processes: (i) collection and processing of STR DNA fragment data; (ii) interpretation of DNA data into DNA profiles used for comparison purposes. At the end of all processes, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and known reference DNA profiles. Statistical weight is provided for all inclusion comparisons.

The technology within the scope of this Biometric Technology Use Policy includes:

Digestion / Extraction

- **Aurora Biomed**: Versa 1100 liquid handler instrument and VERSAware software for automated cell digestion and microscope slide preparation.
- **Qiagen:** EZ1 Advanced XL instrument, EZ2 instrument and Investigator Protocol (Software) for extraction and purification of DNA.

DNA Quantitation

- **Qiagen:** QIAgility Liquid Handler Robots and computers for rapid, high-precision automated PCR setup (also used for Normalization/Amplification and DNA Typing).
- **Applied Biosystems**: QuantStudio 5 Real Time PCR systems and QuantStudio 5 System Detection Software for determination of quantity and quality (degradation level) for a DNA sample.

DNA Normalization / Amplification – STR (autosomal and Y)

- **ThermoFisher Scientific**: SpeedVac DNA Concentrator for concentrating low quantity DNA samples.
- **ThermoFisher Scientific**: ProFlex Thermalcyclers for PCR amplification of STR DNA fragments.

DNA Typing – STR (autosomal and Y)

- **ThermoFisher Scientific**: Applied Biosystems 3500 Series Genetic Analyzer and Data Collection Software is designed for data collection in human identification (HID) applications. The Crime Laboratory uses/intends to use this software to collect STR DNA data from amplified samples. This software normalizes genetic data and creates "hid" files to be used by data processing (FaSTR) and interpretation (ArmedXpert, STRmix) software.

DNA Interpretation – STR (autosomal and Y)

- **NicheVision**: FaSTR software is used for review and evaluation of sizing and genotyping data generated from the genetic analyzers. This analysis software can be configured to set analysis parameters, edit raw data, and aids to prepare data for further interpretation into DNA profiles.
- **NicheVision**: ArmedXpert Analysis Software is used for streamlined DNA typing interpretation resulting in reduced time spent on DNA mixture interpretation. It also uses published and validated population DNA allele frequencies to calculate DNA profile frequency estimates to aid in providing the weight of any inclusion comparison drawn between an evidence sample and a known reference.
- **NicheVision**: STRmix™ software combines established and validated biological modelling and complex mathematical processes to use a continuous model to interpret a wide range of complex DNA profiles. It can compare these DNA profiles to a reference profile and calculate the weight of the comparison using well established Likelihood Ratio statistics.

DNA Databasing

- **HP**: Server for the Combined DNA Index System (CODIS) and peripheral computers used to enter and search evidence DNA profiles against legally obtained reference samples (Convicted Offenders, Arrestees, Missing Persons) and other evidence profiles.

The forensic evidence analyzed by the Forensic Biology Unit develops biometric data, however, the Department does not use it in a surveillance capacity (prospectively), it uses it to solve crimes that have already occurred (retrospectively).

The Forensic Biology/DNA Unit focuses most analytical efforts on violent crimes. Homicides and most sexual assault crimes do not have a statute of limitations. The unit analyzes a wide range of other crime types: robberies, burglaries, thefts, assault, weapons, which may have statute of limitations; however, legal enhancements of penalties (for example 209 PC, aggravated kidnapping) exist, so a 211 PC can be enhanced to a life sentence. It is not the purview of the laboratory to determine the legal status of cases. Laboratory-generated evidence may be used in criminal or civil proceedings. Federal Rules of Civil Procedure 37(e) imparts a duty to preserve potentially relevant evidence including electronically stored information (ESI) for civil trials.

2. Authorized Use

The DNA instrumentation and analysis software described above shall be used primarily on evidence or reference samples submitted by law enforcement and collected pursuant to a search warrant, other legal means, or by documented consent. The DNA instrumentation and analysis software shall be used solely for aiding in criminal or civil investigations; for validating new methods and for special projects designed to evaluate improvements to the forensic DNA collection and analysis process, collecting data for statistical studies or lecture presentations; and for quality assurance purposes. To the latter, reference samples from Crime Laboratory staff members, staff family members, interns, and OPD personnel who

have access to evidence from crime scenes, property storage areas, or the operational areas of the Crime Lab may be processed using the DNA instrumentation and analysis software. This is necessary as a part of the chain of processes used to develop DNA profiles to measure or detect a contamination event in the unit, should it occur. All other uses are prohibited.

The DNA instrumentation and analysis software shall not be used for personal, non-law-enforcement-related purposes; and shall not be used to surveil, harass, intimidate, or discriminate against any individual or group. The Criminalistics Division and Forensic Biology/DNA unit each maintain manuals [Laboratory Operations and Quality Assurance Manual (LOQAM) and standard operating procedures (SOP)] to which all Forensic Biology/DNA unit staff train annually and are required to adhere. LOQAM and the Forensic Biology/ DNA unit SOPs provide rules and procedures on what elements shall be present in a validation study, data and conclusions from validation studies performed, rules on conducting research and any published results. Failure to follow these rules and procedures may result in discipline.

3. Data Collection

The data collected attests to the purity or amount of the DNA and usually also contains genetic information, specifically STR DNA marker alleles (types) that collectively constitute a forensic DNA profile that has the potential to characterize or identify a single individual. (Note: identical twins typically have identical forensic DNA profiles, since they are derived from a single fertilized egg, or zygote).

The Forensic Biology unit maintains an in-house Quality Control (QC) database. The QC database contains DNA profiles obtained from the following sources:

1. by consent from OPD staff (current and past) and their family members.
2. OPD personnel that may enter the chain of custody for an evidence item or has other contact within the scope of the case,
3. Samples provided by accredited proficiency test providers. The samples are anonymized by the test provider; the test providers are subject to strict confidentiality requirements by the accrediting bodies. The laboratory has no access to the source of these samples.

The purpose and use of the QC database is twofold: 1) for casework quality control checks to ensure that the process worked correctly (positive control) and 2) to determine if there is possible contamination from a known individual to a casework sample. At this time, there are no victim references in the QC database. Such profiles have never been, nor are they allowed to be, used for the identification of an individual in a criminal matter. Further clarification: no victim DNA profiles can be entered or used in the QC database.

4. Data Access

Criminalists and Forensic Technicians with duties in the Forensic Biology/DNA unit shall be the only Crime Laboratory personnel authorized to use the DNA instrumentation and analysis software in casework, and only after completing a comprehensive training program and qualifying test, at which time, with the Supervisor's recommendation, the Crime Laboratory Manager issues a written authorization. No one else shall have the authority to grant access to use DNA instruments or software in casework. Criminalists and Forensic Technicians are granted access to one another's cases only for the purpose of discovery or CPRA requests, documenting quality checks, verifications or peer review. Interns also are authorized to use the DNA instrumentation and analysis software for special projects, not casework, and only after receiving necessary training and under the supervision of a qualified Criminalist.

5. Data Protection

All data generated using the DNA instrumentation and analysis software shall be securely maintained at all times in a limited access location, or on a secure server*. To evaluate and interpret the DNA analytical data, authorized personnel shall only use computers on secure network drives.

* The Laboratory's remote server, which hosts network drives, is secure because it is physically under lock and key and limits electronic access to current laboratory staff and ITD personnel. Additionally, a separate local server is secured by lock and key during business and after hours, alarm after hours and by running the server on a dedicated intranet line that uses encryption on both the sender and receiver ends of any communication from/to the server. NOTE: The use of the term "secure servers" or "secure network" throughout this Use Policy is on the basis of working with the Information Technology Department (ITD) in 2020 to develop terminology in this document. ITD is responsible for the preservation, fidelity and security of the data described herein.

6. Data Retention

There is no statute of limitations on most of the cases the Forensic Biology/DNA unit analyzes. For crime types that do have statute of limitations, penalty enhancements may make it such that a decision to impose a life sentence may be rendered and civil duty to preserve ESI and electronic evidence exists; therefore, data are retained indefinitely on secure server or network drives. No hard drive leaves laboratory custody without ensuring that all sensitive data has been removed and is irretrievable from the device. Hard copies of case files containing the laboratory report, notes, and instrument printouts are similarly retained indefinitely under Crime Lab control with secure, limited-access areas, or at a Departmentally approved Records Retention facility. Retained data may be used if questions pertaining to the case in question arise, or if an investigation into a quality issue arises and is documented in Incident Response.

7. Public Access

Members of the public shall have no direct access to the DNA instrument data generated. If requested under the California Public Records Act (CPRA), the Crime Lab shall deny the request on the ground that such data is exempt from disclosure under the investigative exemption (Government Code section 6254(f), (k) and 6255), Evidence Code Section 1040 and perhaps other exemptions, unless and until they are made publicly available in criminal proceedings. If such a CPRA request is made or if a subpoena or court order is issued for such DNA instrumentation and analysis data, the data shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Oakland City Attorney's Office as needed. Criminal defendants are entitled access to the data via third-party data-sharing described in the next section.

8. Third-Party Data-Sharing

Following the completion and review of a specific case, the case file and data are disseminated only to the law enforcement customer and/or City Attorney and/or prosecuting attorney and assisting staff. The material shall be subject to discovery in criminal or civil proceedings and is the means by which criminal defendants are entitled to obtain a copy of the casefile and the data contained therein. The case file and data (including copies) shall not be shared with anyone else without a court order. In addition, crime scene samples that qualify for search in the California State DNA Index System (SDIS) and National DNA Index System (NDIS) (components of the Combined Index System or CODIS database), are uploaded to SDIS according to the NDIS Operational Procedures Manual (https://www.fbi.gov/file-repository/ndis-operational-procedures-manual.pdf/view). Suspect DNA profiles that qualify for search are uploaded to SDIS pursuant to California Penal Code 297.

Accessing data collected by the Forensic Biology/DNA unit requires either a right to know or a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law (covered in Section 4. Data Access). A need to know is a compelling reason to request information such as being the OPD Investigator assigned to the case for which DNA analysis has been requested.

Forensic Biology/DNA data may be shared only with other law enforcement agencies based on a need to know and a right to know, or as otherwise required by law, using the following procedures:

1. The agency makes a written request for the Forensic Biology/DNA data that includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The need for obtaining the information.

2. The request is reviewed by the Bureau of Investigation Deputy Chief or designee and is approved before the request is fulfilled.

3. The approved request is retained on file, and shall be included in the annual report

9. Training

Forensic Technicians and Criminalists in the Forensic Biology/DNA unit shall complete a comprehensive training program and shall not embark on any casework with the DNA instrumentation and analysis software until they have successfully taken a relevant qualifying test. Once qualified, they shall take proficiency tests bi-annually. Interns shall be authorized to use the DNA instrumentation and analysis software for special projects, and not casework, only after receiving necessary training and under the supervision of a qualified Criminalist. Criminalists, Forensic Technicians, and interns in the Forensic Biology/DNA unit shall be provided with a copy of the DNA instrumentation and analysis software Biometric Technology Use Policy. The Crime Lab Manager and Criminalist IIIs are responsible for providing oversight of the training program, ensuring comprehension of policies and documenting adherence.

10. Auditing and Oversight

The Forensic Biology/DNA unit is overseen by two supervisors and by Crime Lab upper management (Crime Lab Manager and Quality Supervisor), all of whom shall oversee compliance with this Biometric Technology Use Policy and Standard Operating Procedures via Administrative and Quality Reviews of casework, policy updates and annual Internal Audits. Additionally, the Crime Lab is accredited by the American National Standards Institute (ANSI) National Accreditation Board (ANAB), which provides oversight to the operation of the Forensic Biology Unit. The Crime Lab is assessed by ANAB on an annual basis. Moreover, the Forensic Biology/DNA unit complies with the Federal Bureau of Investigation (FBI)'s Quality Assurance Standards (QAS) for Forensic DNA Testing Laboratories. The Forensic Biology unit is audited to the FBI's QAS annually, alternating internal and external audits.

11. Maintenance

The mechanism to ensure the security and integrity of the tools, instrumentation and data are insured by oversight provided by the Forensic Biology/DNA unit Supervisors and upper management as defined in the "Auditing and Oversight" section above.