Surveillance Technology Policy

Verogen MiSeq DNA Sequencing Instrument
Police Department

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Verogen MiSeq DNA Sequencing Instrument itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

In order protect life and property, prevent crime and reduce the fear of crime, we will provide service with understanding, response with compassion, performance with integrity and law enforcement with vision.

The Surveillance Technology Policy ("Policy") defines the manner in which the Verogen MiSeq DNA Sequencing Instrument will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Verogen MiSeq DNA Sequencing Instrument, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of Verogen MiSeq DNA Sequencing Instrument technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

Generate sequenced DNA profiles from evidence to search against databases of evidence and reference samples for the purpose of accurately and expeditiously identifying, apprehending, arresting, and convicting criminal offenders and exonerating persons wrongly suspected or accused of crime or to identify human remains.
Generate sequenced DNA profiles from submitted reference samples for direct comparison to evidence samples for the purpose of accurately and expeditiously identifying, apprehending, arresting, and convicting criminal offenders and exonerating persons wrongly suspected or accused of crime or to identify human remains.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

DNA profiles do not reveal political opinions, religious or philosophical beliefs, or trade union membership or sexual orientation.

BUSINESS JUSTIFICATION

Verogen MiSeq DNA Sequencing Instrument supports the Department's mission and provides important operational value in the following ways:

The SFPD crime lab generates sequenced DNA profiles from evidence samples left at crime scenes and reference samples submitted to the lab. Direct comparisons of evidence to reference samples are made, in additional, evidence DNA profiles can be entered into databases such as CODIS (FBI's Combined DNA Index System) for searching to identify potential matches.

The Department has compelling interest in the accurate identification of criminal offenders.
In addition, Verogen MiSeq DNA Sequencing Instrument promises to benefit residents in the following ways:

☐	Education	
☐	Community Development	
☐	Health	
☐	Environment	
✠	Criminal Justice	efficiently generate comprehensive and useful data from biological evidence collected at a crime scene to aid the forensic DNA analysis, related criminal investigations and close more criminal cases
☐	Jobs	
☐	Housing	
☐	Other	

Verogen MiSeq DNA Sequencing Instrument will benefit the department in the following ways:

Benefit		Description	Quantity
☑	Financial Savings	Forensic DNA sequencing analysis can focus an investigation and eliminate unnecessary staffing costs	
☑	Time Savings	Forensic DNA sequencing analysis can focus an investigation and eliminate unnecessary investigation	
☐	Staff Safety		
☑	Data Quality	Forensic DNA sequencing analysis provides investigators with information grounded in science and is proven to be reliable.	
☐	Other		

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

<table>
<tr><td>Specifications:</td><td>The software and/or firmware used to operate the surveillance technology must be kept up to date and maintained.</td></tr>
<tr><td>Safety:</td><td>Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.</td></tr>
<tr><td>Data Collection:</td><td>Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

Data types can take the form video, audio, still images. Data formats can take the form of XML, PDF, HTML, Plain Text, JPEG, etc. The surveillance technology collects the following data types and formats:

• Video in MOV format
• Still images from cameras in PDF format

The surveillance technology collects the following data types:

<table><tr><th>Data Type(s)</th><th>Format(s)</th><th>Classification</th></tr><tr><td>DNA sequence</td><td>Miseq file</td><td>Level 3</td></tr></table></td></tr>
<tr><td>Notification:</td><td>This equipment will only be in use at the SFPD Crime Lab. The Department will include the name of this technology on its surveillance technology inventory website page found here: https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies</td></tr>
<tr><td>Access:</td><td>All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below): Results of forensic DNA sequence analysis and any database matches are reported to the SFPD investigator who submitted the request for analysis.

Instrument data is only available to lab personnel.</td></tr>
</table>

	A. Department employees Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology. • Criminalist 8259 – 8262, DNA Technical Leader Manager, Crime Lab Manager (0933), SFPD Crime Lab The following providers are required to support and maintains the surveillance technology and its associated data to ensure it remains functional: • Yes – eligible DNA profiles are maintained in the FBI CODIS database for searching against DNA profiles across the United States on the Criminal Justice Information Services Division Wide Area Network (CJIS-WAN). *B. Members of the public* Forensic DNA data is classified as Level 3 Sensitive. California Penal Code 299.5 (b) "All evidence and forensic samples containing biological material retained by the Department of Justice DNA Laboratory or other state law enforcement agency are exempt from any law requiring disclosure of information to the public or the return of biological specimens, samples, or print impressions*".*
Data Security:	Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s). To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards: Data is restricted to lab personnel. The lab network is password protected and controlled by SFPD IT. The physical access to the lab is restricted to lab personnel and DNA lab space is restricted to DNA lab personnel.
Data Sharing:	Police will endeavor to ensure that other agencies or departments that may receive data collected by MiSeQ DNA Sequencer will act in conformity with this Surveillance Technology Policy. For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

	Police shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security) Each department that believes another agency or department receives or may receive data collected from its use of STs should consult with its assigned deputy city attorney regarding their response. Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place: ☑ Confirm the purpose of the data sharing aligns with the department's mission. ☐ Consider alternative methods other than sharing data that can accomplish the same purpose. ☐ Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies. ☑ Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents. ☑ Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance. ☐ Ensure shared data will be done in a cost-efficient manner and exported in a clean, machine-readable format. The Department currently participates in the following sharing practices in accordance with the DNA Identification act of 1994: A. Internal Data Sharing The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco. B. External Data Sharing Department does not share instrument data but an interpreted profile will be shared with the recipient: FBI- The Combined DNA Index System **(**CODIS) database Data sharing occurs at the following frequency: Weekly To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Data is stored indefinitely.

<table>
<tr>
<td>Data Retention:</td>
<td>Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

Please list data retention schedules (i.e., x type of data will be retained for 1 year) based on the following categories:
• Permanent records (i.e., records that are essential): shall be retained and preserved indefinitely
• Current records (i.e., records for operational necessity, ready reference, convenience): record retention schedules may vary but generally less than 10 years
• Storage records (i.e., records retained offsite): record retentions may vary but generally less than 10 years

The Department’s data retention period and justification are as follows:
<table>
<tr><td>Data is stored indefinitely.</td><td>allows for any appeals process to occur or if further analysis is needed it will be available and for samples to remain in the CODIS database for searching (DNA Identification Act 1994).</td></tr>
</table>
Data will be stored in the following location:

☑ Local storage
☐ Department of Technology Data Center
☐ Software as a Service Product
☐ Could Storage Provider</td>
</tr>
<tr>
<td>Data Disposal:</td>
<td>Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices: n/a

Processes and Applications: n/a</td>
</tr>
<tr>
<td>Training:</td>
<td>To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or</td>
</tr>
</table>

	regularly requiring data access receive appropriate training before being granted access to systems containing PII. Per DNA quality assurance standards, all analysts must complete a documented training program and be authorized by the DNA Technical leader before performing casework and accessing data.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

These policies will have the same compliance requirements as all Department Written Directives and Police Commission Resolutions.

The Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties. Director of SFPD Crime Lab, Deputy Chief of Investigations, Assistant Chiefs and Chief of Police.
In addition, each member of the department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD written directives and the surveillance technology polices. If allegations arise that a member is not in compliance, the OIC will initiate an investigation and will take the appropriate action which could include an investigation of misconduct by Internal Affairs.

Sanctions for violations of this Policy include the following:

San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA may elect to file charges with the Police Commission for any penalty greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

If the Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

The Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

DEFINITIONS

Personally Identifiable Information:	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Raw Data:	Information collected by a surveillance technology that has <u>not</u> been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.

Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Public:

Complaints of Officer Misconduct: Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA). DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD. DPA manages, acknowledges and responds to complaints from members of the public.

Concerns and Inquiries: Department shall acknowledge and respond to concerns in a timely and organized response. To do so, the Department has included a 19B Surveillance Technology Policy page on its public website : https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies. This page includes and email address for public inquiries: SFPDChief@sfgov.org. This email is assigned to several staff members in the Chief's Office who will respond to inquiries within 48 hours.

Allegations of 19B Violations: Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org. If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation. The Department will comply with allegation and misconduct processes as set forth by the City Charter.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

The Verogen MiSeq system performs sequencing of DNA from evidence and reference samples needed for comparison. The technology used is massively parallel sequencing allowing for more information from highly degraded samples and mixed DNA samples. Below are the components of the system:
Verogen MiSeq and accompanying reagents – Massively Parallel sequencing instrument – used on samples that yield no results or no CODIS matches when attempted with Life Technology instruments and accompanying reagents.

ForenSeq Universal Analysis Software – software to analyze DNA sequencing results

The MiSeq FGx System is the first and only next-generation sequencing (NGS) instrument developed and validated for forensic genomics. Combining proven data quality with ease of use, the system is the key to a unique, single-platform solution built on gold-standard NGS technology. Prepare and sequence libraries and analyze data in a single workflow designed to scale for a growing portfolio of applications, including new tools like forensic genetic genealogy (FGG). Dedicated reagent kits and matched analysis software empower answers for all human identification cases.

Backed by validation and implementation services, the MiSeq FGx System is a compact, bench-top platform that saves valuable laboratory space. The first and only instrument to interrogate SNPs and STRs in a single run, the MiSeq FGx System preserves precious sample while demonstrating robust performance. Develop more thorough, detailed DNA profiles from a wide range of sample types, from high-quality genomic DNA (gDNA) to degraded, mixed, and limited samples.
Specifications:
Power requirements 100–240 VAC at 50/60 Hz, 10A, 400 W
RFID radio frequency 13.56 MHz
RFID power 100 mW
Dimensions 68.6 cm × 56.5 cm × 52.3 cm (27 in × 22.2 in × 20.6 in)
Weight 54.5 kg (120 lbs)

https://verogen.com/wp-content/uploads/2018/07/MiSeq-FGx-forensic-genomics-solution-data-sheet-VD2018003.pdf

FBI-DOJ

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

Technology Use:

The SFPD crime lab generates sequenced DNA profiles from evidence samples left at crime scenes and reference samples submitted to the lab. Direct comparisons of evidence to reference samples are made, in additional, DNA profiles can be search and/or entered into databases such as CODIS (FBI's Combined DNA Index System) to identify potential matches.

PII:

true

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.

Authorized Uses:

Generate sequenced DNA profiles from evidence to search against databases of evidence and reference samples

Generate sequenced DNA profiles from submitted reference samples for direct comparison to evidence samples

Rules:

Prohibited Uses:

Data is only available to lab personnel.

4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed.

Data Type	Formats STP
DNA sequence	.Miseq file

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.

Employee Job Classification & Title:

Data is only available to lab personnel.

Department:

SFPD Crime Lab

If applicable, contractor or vendor name:

n/a

Rules and processes required prior to data access or use:

Data is restricted to lab personnel. The lab network is password protected and controlled by SFPD IT. The physical access to the lab is restricted to lab personnel and DNA lab space is restricted to DNA lab personnel.

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.
Data is only available to lab personnel.
7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period
Retention: allows for any appeals process to occur or if further analysis is needed it will be available. Reason for retention: n/a Deletion process: allows for any appeals process to occur or if further analysis is needed it will be available. Retention exemption conditions: n/a
8. How collected information can be accessed or used by members of the public, including criminal defendants
Will the data be accessible to the public: Data is stored indefinitely. How it can be accessed:
9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.
Name of agency: FBI- CODIS database Justification: https://oig.justice.gov/reports/FBI/a0126/intro.htm *"A core function of the Department of Justice is solving crime, which includes aiding state and local law enforcement agencies to do the same. On an increasing basis, the use of DNA profiles (a computerized record containing DNA characteristics used for identification) has aided their effort. To further the use of DNA in solving crime, the Federal Bureau of Investigation (FBI) created a hierarchy of DNA profile indexes, the Combined DNA Index System (CODIS). CODIS is a national DNA information repository maintained by the FBI that allows state and local crime laboratories to store and compare DNA profiles from crime-scene evidence and convicted offenders. The goal of the system is to match case evidence to other previously unrelated cases or to persons already convicted of other crimes".*

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Training required:

true

Description of training:

Per DNA quality assurance standards, all analysts must complete a documented training program and be authorized by the DNA Technical leader before performing casework and accessing data.

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Training required:

true

Process for responding to complaints:

n/a

Oversight process:

San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the DPA. Depending on the severity of the allegation of misconduct, the Chief or the DPA may elect to file charges with the Police Commission for any penalty greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

Compliance personnel titles:

Criminalist 8259 – 8262, DNA Technical Leader Manager, Crime Lab Manager (0933), SFPD Crime Lab

Restrictions:
Data is only available to lab personnel.

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaint procedures:

Complaints of Officer Misconduct: Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA). DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD. DPA manages, acknowledges and responds to complaints from members of the public.
Concerns and Inquiries: Department shall acknowledge and respond to concerns in a timely and organized response. To do so, the Department has included a 19B Surveillance Technology Policy page on its public website :

https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies. This page includes and email address for public inquiries: SFPDChief@sfgov.org. This email is assigned to several staff members in the Chief's Office who will respond to inquiries within 48 hours.

Allegations of 19B Violations: Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org. If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation. The Department will comply with allegation and misconduct processes as set forth by the City Charter.

City and County of San Francisco Employees:
All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org

Departmental follow-up process:

These policies will have the same compliance requirements as all Department Written Directives and Police Commission Resolutions.
The Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties. Director of SFPD Crime Lab, Deputy Chief of Investigations, Assistant Chiefs and Chief of Police.
In addition, each member of the department belongs to a chain of command. The Officer in Charge (OIC) of that chain of command is responsible for overseeing compliance with all SFPD written directives and the surveillance technology polices. If allegations arise that a member is not in compliance, the OIC will initiate an investigation and will take the appropriate action which could include an investigation of misconduct by Internal Affairs.

Members of the public can register complaints/concerns or submit questions via calls or emails at 311.org.