

VIRGINIA STATE POLICE &
DEPARTMENT OF CRIMINAL
JUSTICE SERVICES

Facial Recognition
Technology

**Guide for Agency Reporting
Requirements**

Version 1.0
Effective January 1, 2023

Contents

Background	3
Data Required	3
Reporting Requirements	4
Definitions	5
<hr/>	
Record Level Data – Query Characteristics	7
<hr/>	
Record ID	
Query Date	
Host Agency ORI	
Test Case Flag	
Host Agency Case Number	
User ID	
Other Agencies Shared	
Requestor Agency ORI	
Requestor Case Number	
Authorized Use Type	
Criminal Offense Type	
Gang/Riot Related Activity	
Nature of Repository	
Subject Race	
Subject Ethnicity	
Subject Gender	
<hr/>	
Record Level Data – Query Outcomes	13
<hr/>	
List of Possible Candidates	
Examiner Offered Investigative Lead	
Case Closed Involving Investigative Lead	
<hr/>	
Data File Submission Process	15
<hr/>	
File Extraction	
File Naming Convention	
File Submission to DCJS	
File Requirements	
Reporting “No Queries” (Zero Report)	
Process Diagram	
<hr/>	
Appendix A: FRT Use Record Structure Example	17
<hr/>	

Background

The 2022 session of the General Assembly passed SB 741 to amend and reenact §§ 15.2-1723.2 and 23.1-815.1 of the Code of Virginia and to add a section numbered § 52-4.5, authorizing Virginia law enforcement agencies to use facial recognition technology (FRT) for investigative purposes until the expiration date of July 1, 2026. The bill mandates that all law enforcement agencies who use FRT must annually publish certain FRT use metrics by April 1 of each year. This FRT Guide for Agency Reporting Requirements document outlines the metrics and reporting standards for those mandated FRT use requirements.

Data Required

§ **15.2-1723.2**. Facial recognition technology; approval; penalty¹.

E. Any local law-enforcement agency that uses facial recognition technology shall maintain records sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting, and auditing of compliance with such agency's facial recognition technology policies. Such agency shall collect data pertaining to (i) a complete history of each user's queries; (ii) the total number of queries conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how many times an examiner offered law enforcement an investigative lead based on his findings; (v) how many cases were closed due to an investigative lead from facial recognition technology; (vi) what types of criminal offenses are being investigated; (vii) the nature of the image repository being compared or queried; (viii) demographic information for the individuals whose images are queried; and (ix) if applicable, any other entities with which the agency shared facial recognition data.

F. Any chief of police whose agency uses facial recognition technology shall publicly post and annually update a report by April 1 each year to provide information to the public regarding the agency's use of facial recognition technology. The report shall include all data required by clauses (ii) through (viii) of subsection E in addition to (i) all instances of unauthorized access of the facial recognition technology, including any unauthorized access by employees of the agency; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable, data or links related to third-party testing of such algorithms, including any reference to variations in demographic performance. If any information or data (a) contains an articulable concern for any person's safety; (b) is otherwise prohibited from public disclosure by federal or state statute; or (c) if disclosed, may compromise sensitive criminal justice information, such information or data may be excluded from public disclosure. Nothing herein shall limit disclosure of data collected pursuant to subsection E when such disclosure is related to a writ of habeas corpus.

¹ Subsections E and F of §§ 23.1-815.1 and 52-4.5 are identical to this text, except for reference to campus police departments and Department of State Police respectively as the agencies using facial recognition technology.

For purposes of this subsection, "sensitive criminal justice information" means information related to (1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source, or (3) law-enforcement investigative techniques and procedures.

Reporting Requirements

Per the Facial Recognition Technology (FRT) model use policy, law enforcement agencies using Facial Recognition Technology are required to follow reporting standards outlined in this document in addition to the requirements in the Code of Virginia (reprinted in the "Data Required" section of this document). Any agency using Facial Recognition Technology who does not follow these reporting standards is considered non-compliant with the FRT model use policy.

In addition to submitting FRT metrics data to the Department of Criminal Justice Services (DCJS), your agency must publicly post all aggregated metrics listed in Sections E (excepting item *i*) and F of the relevant code section (§ 15.2-1723.2, 23.1-815.1, or 52-4.5) by April 1 of each year (with data covering the full preceding calendar year). Section E metrics are reported using the FRT Record-Level Data Template, and Section F metrics are reported via the FRT Annual Agency-Level Data Form.

Record-Level Data

The mandate for the DCJS report includes analysis and recommendations for "improving the use of facial recognition technology as it relates to demographics associated with race, skin tone, ethnicity, and gender" based on the metrics reported by law enforcement agencies. While the compliance metrics requirements for law enforcement agencies are structured as aggregated totals in the statute, DCJS requires disaggregated record-level data to analyze FRT use trends related to subject demographics. Law enforcement agencies using FRT are responsible for submitting a record for every FRT query performed by the agency that year.

Annual Agency-Level Data

Some of the metrics mandated in the FRT use statute are not linked to specific FRT queries or their outcomes. These metrics are outlined in the FRT Annual Agency-Level Data Form to be submitted by April 1 of each year. The form should only be completed once per year for each agency using FRT, and all information provided should cover the full preceding calendar year. Refer to the instructions within the FRT Annual Agency-Level Data Form for details on submitting these metrics.

Definitions

Authorized Use

Code of Virginia § 15.2-1723.2(A)

"Authorized use" means the use of facial recognition technology to (i) help identify an individual when there is a reasonable suspicion the individual has committed a crime; (ii) help identify a crime victim, including a victim of online sexual abuse material; (iii) help identify a person who may be a missing person or witness to criminal activity; (iv) help identify a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife; (v) help identify an online recruiter of criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking; (vi) help a person who is suffering from a mental or physical disability impairing his ability to communicate and be understood; (vii) help identify a deceased person; (viii) help identify a person who is incapacitated or otherwise unable to identify himself; (ix) help identify a person who is reasonably believed to be a danger to himself or others; (x) help identify an individual lawfully detained; (xi) help mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism; (xii) ensure officer safety as part of the vetting of undercover law enforcement; (xiii) determine whether an individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or other official forms of identification using information that is fictitious or associated with a victim of identity theft; or (xiv) help identify a person who an officer reasonably believes is concealing his true identity and about whom the officer has a reasonable suspicion has committed a crime other than concealing his identity.

Facial Recognition Technology

Code of Virginia § 15.2-1723.2(A)

"Facial recognition technology" means an electronic system or service for conducting an algorithmic comparison of images of a person's facial features for the purpose of identification. "Facial recognition technology does not include the use of an automated or semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the recording prior to release or disclosure of the recording outside of the law-enforcement agency if the process does not generate or result in the retention of any biometric data or surveillance information."

Host Agency

The agency performing a facial recognition query. A host agency may either perform a query for their own purposes, or they may share the query results with a Requesting Agency.

Query

For the purposes of this document, “query” refers to the full set of facial recognition searches run on the same day for the same subject. Each query requires its own record for facial recognition use reporting and is composed of one or more Searches.

Requesting Agency

Any agency which requests that another Virginia law enforcement agency perform a facial recognition query on their behalf. For queries requested by a multi-agency task force, the requesting agency would be Virginia State Police (or the Federal Bureau of Investigation for federal task forces).

Search

For the purposes of this document, “search” refers to each instance that a user checks a probe image against an image repository. Each search is part of a Query.

Explanation of Record Structure – “Query” versus “Search”

To accommodate the Code’s requirements without creating an excessive reporting burden, DCJS and VSP have structured the FRT use data reporting elements to capture Queries as composed of one or more Searches of the same subject on the same day. The Query serves as a meaningful unit of actual investigative efforts to perform facial recognition of a subject, while tracking Searches allows each agency to track and report the total use volume of their facial recognition system.

To properly report your agency’s facial recognition use data, create a new record **per Query** based on a set of **Searches** for the same subject on the same day. Note that this means a case involving Searches of two different subjects would be reported as two separate **Queries**, each one noting the case number for reference. A case in which 4 probe images of the same subject are checked against the repository on the same day would be one **Query** record composed of 4 **Searches**. See Appendix A for an example on how one case’s searches would be structured into query records.

Record-Level Data Elements

The following data elements pertain to the variables contained in the FRT Record-Level Data Template. Each element must be filled out for each query record according to the instructions below.

Record-Level Data Elements: Query Characteristics

Record ID

A unique record identifier for each submitted **query** assigned by the reporting agency to uniquely identify the query.

Format: Up to 30-Character Alphanumeric (ex. 1234)

Must contain a valid character combination of the following:

- A–Z (capital letters only)
- 0–9
- Period (.), Hyphen (-), Parenthesis (), At symbol @, Slash (/)
- No commas

Query Date

Indicate the date of the query. **Do not include a timestamp.**

If entering manually on the table, include forward slash (/). Date will convert to MMDDYY when tab to the next field.

Format: 6-Character Numeric (MMDDYY)

Number of Searches

Enter the number of searches performed for this query. Note that for auditing purposes, this field will help to reconcile differences between the query count and the number of individual searches performed.

Format: Numeric (Value 1 or greater)

Host Agency ORI

Indicate the primary 9-digit ORI assigned to the agency making the query.

[Virginia ORI Codes](#)

The ORI for your agency is available on the listed VCIN or IBR list. If your agency does not have an ORI, please let our office know via email.

Format: 9-Character Alphanumeric (VAVSP0000)

Must contain a valid character combination of the following:

- A–Z (capital letters only)
- 0–9

Test Case Flag

If this query is being performed purely for system testing and/or training purposes and IS NOT connected to any police investigation, select “Yes” for this option. You do not need to complete any other data elements for Test Cases. Note that cases marked as Test Cases will be audited to ensure that they were legitimately performed as test or training queries rather than unauthorized or unreported investigative queries.

- Yes (Do not complete any further data elements)
- No

Host Agency Case Number

Enter the host agency’s case number associated with the query. **This case number should be used to track query outcomes data per the FRT Use Policy.**

Subject ID

Enter the ID for the query subject using the format *RoleX*, where *Role* is the subject type (either “Suspect” for criminal suspect or “Other” for any other subject not under criminal suspicion) and *X* is a sequential number to distinguish between subjects of the same type within the same case. For example, in a case involving two different suspects who are queried, the Subject IDs would be “Suspect1” and “Suspect2” and a separate record would be created for each suspect.

User ID

A unique record identifier for each user who ran queries at your agency. Be sure to retain a departmental key linking each user to their User ID, and consistently use the correct ID with each user in your record set. Do not use publicly identifiable IDs such as badge numbers or employee IDs.

Format: Up to 10-Character Alphanumeric (ex. 1234)

Must contain a valid character combination of the following:

- A–Z (capital letters only)
- 0–9
- Period (.), Hyphen (-), Parenthesis (), At symbol @, Slash (/)
- No commas

Other Agencies with which Facial Recognition Data was Shared

Indicate whether this query was performed per another law enforcement agency’s request. If yes, provide the name of the agency.

- Yes (Please Specify)
- No

Requestor ORI

If this query was performed per another law enforcement agency's request, indicate the primary 9-digit ORI assigned to the agency requesting the query.

[Virginia ORI Codes](#)

For all Virginia agencies, the agency ORI is available on the listed VCIN or IBR list. If an out of state requestor agency does not have an ORI, please notify the DCJS facial recognition contact at FRTdata@dcjs.virginia.gov.

Format: 9-Character Alphanumeric (VAVSP0000)

Must contain a valid character combination of the following:

- A–Z (capital letters only)
- 0–9

Requestor Case Number

Enter the requesting agency's case number associated with the query. **This case number should be used to track query outcomes data per the FRT Use Policy.**

Authorized Use for Query

Based on the 14 uses outlined in the Virginia Code, indicate the **Authorized Use** which applies to the query. If multiple authorized uses apply for the query, select the most precise value (for example, record a query of a human trafficking victim under #4 for Trafficking Victim rather than #2 for Crime Victim). **Only data values below accepted. If you are unable to identify the use type for a given query, that query must be reported as an unauthorized use.**

Format: Up to 2-Character Numeric

Values: Applicable values below

Valid Data Values	Value Name	Statutory Description
1	Criminal Investigation - Reasonable Suspicion	Help identify an individual when there is a reasonable suspicion the individual has committed a crime
2	Crime Victim	Help identify a crime victim, including a victim of online sexual abuse material
3	Missing Person/Witness	Help identify a person who may be a missing person or witness to criminal activity

4	Trafficking Victim/Individual	Help identify a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife
5	Online Recruiter	Help identify an online recruiter of criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking
6	Mental/Physical Disability	Help a person who is suffering from a mental or physical disability impairing his ability to communicate and be understood
7	Deceased Person	Help identify a deceased person
8	Incapacitated/Unable to Identify	Help identify a person who is incapacitated or otherwise unable to identify himself
9	Danger to Self/Others	Help identify a person who is reasonably believed to be a danger to himself or others
10	Lawfully Detained	Help identify an individual lawfully detained
11	Mitigate Threat	Help mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism
12	Undercover Officer	Ensure officer safety as part of the vetting of undercover law enforcement
13	Unlawful/Fictitious Identification	Determine whether an individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or other official forms of identification using information that is fictitious or associated with a victim of identity theft
14	Concealed ID - Reasonable Suspicion	Help identify a person who an officer reasonably believes is concealing his true identity and about whom the officer has a reasonable suspicion has committed a crime other than concealing his identity

Criminal Offense Type

Identify the type of criminal offense(s) being investigated for each query. For queries where no criminal investigation is involved, select N/A.

Acceptable Values (Check all that apply):

- Animal Cruelty/Trafficking
- Arson
- Assault
- Burglary
- Drug – Schedule I or II
- Drug – Other
- Fraud/Identity Theft

- Kidnapping
- Larceny
- Homicide/Manslaughter
- Human Trafficking
- Pornography/Obscenity
- Rape
- Other Sexual Assault
- Robbery
- Terrorism
- Traffic
- Vandalism
- Weapon/Firearm
- Other Criminal Offense (Please Specify)
- N/A, no criminal investigation

Gang/Riot Related Activity

Identify whether suspected gang or riot activity was involved in the query.

- Gang activity
- Participation in/incitement of Riot
- None

Nature of Repository

Identify the nature of the image repository being compared or queried (the “pool” of images used to match your subject image).

Acceptable Values (Check all that apply):

- Mug-shot images
- Driver’s license/Other State Identification photographs
- Sex Offender Registry
- Vendor Database
- Other (Please Specify)

Subject Race

Indicate the race of the Individual queried as stated in a police report (if available) or based on the judgement of the query operator.

Format: 1-Character Alphabetic

Valid Data Values	Description
W	White
B	Black or African American

I	American Indian or Alaska Native
A	Asian or Native Hawaiian or Other Pacific Islander
U	Unknown

The definitions of the racial designations are:

White—A person having origins in any of the original peoples of Europe/Middle East/North Africa

Black or African American—A person having origins in any of the black racial groups of Africa

American Indian or Alaska Native—A person having origins in any of the original peoples of North and South America (including Central America) and who maintains tribal affiliation or community attachment

Asian/Pacific Islander—A person having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam or a person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.

Subject Ethnicity

Indicate the ethnicity of the Individual queried as stated in a police report (if available) or based on the judgement of the query operator.

Format: 1-Character Alphabetic

Valid Data Values	Description
H	Hispanic or Latino
N	Not Hispanic or Latino
U	Unknown

The ethnic designation of Hispanic or Latino includes persons of Mexican, Puerto Rican, Cuban, Central or South American, or other Spanish culture or origin, regardless of race.

Subject Gender

Indicate the gender of the Individual queried as stated in a police report (if available) or based on the judgement of the query operator.

Format: 1-Character Alphabetic

Valid Data Values	Description
F	Female
M	Male
O	Other
U	Unknown

Record-Level Data Elements: Query Outcomes

The following data elements are based on the results of each FRT query. They will require follow-up revisions and updates as each investigation involving a query progresses. **Finalized records should reflect the status of each query's investigation as of the end of the reporting year.**

List of Possible Candidates

Indicate whether the query resulted in a list of possible match candidates.

Format: 1-Character Alphabetic

Valid Data Values	Description
Y	Yes
N	No

Examiner Offered Investigative Lead

Indicate whether an examiner offered law enforcement an investigative lead based on the findings of the query. **If the value for this data element is "Y", the value for the "List of Possible Candidates" element must also be "Y."**

Format: 1-Character Alphabetic

Valid Data Values	Description
Y	Yes
N	No

Case Closed involving Investigative Lead

Indicate whether an examiner offered an investigative lead based on this query, and the same subject (victim, witness, suspect, etc.) was confirmed to be involved when the case was closed.

If the value for this data element is “Y”, the value for the “Examiner Offered Investigative Lead” element must also be “Y.”

Note: Item “v” within Section E of § 15.2-1723.2 directs agencies to report “how many cases were closed due to an investigative lead from facial recognition technology.” However, the causal role of an FRT query lead in closing a case cannot be isolated from other evidence gathered in the course of investigation. Therefore, this “Case Closed Involving Investigative Lead” metric shifts the focus to a more discernable question of whether an individual offered as a lead from an FRT query is later confirmed to be involved in the case being investigated. A “Yes” response to this question does not imply the guilt of any criminal suspect.

Format: 1-Character Alphabetic

Valid Data Values	Description
Y	Yes
N	No
U	Case Still Active/Under Investigation

Data File Submission Process

File Extraction

Record-level query data should be collected throughout the year using the FRT Record-level Data Template. Collected data elements should be submitted by April 1 of each year.

File Naming Convention

The file name should be as follows: **HostORI_FRTRecords_Year**

Example: VA9999999_FRTRecords_2023

File Submission

Once all data has been collected for the year, please email the file to the DCJS data collection address at frtdata@dcjs.virginia.gov.

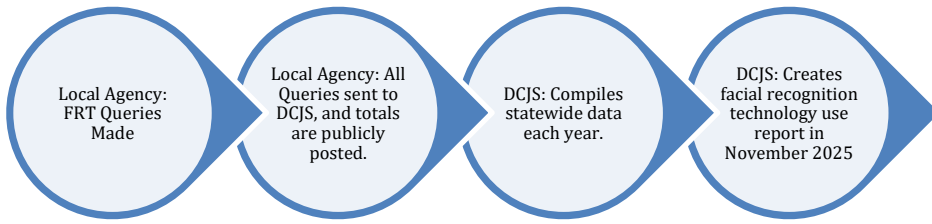
File Requirements

- All record level data must be on **one** tab/sheet titled "Record Level." Annual agency level data should be submitted using the "Annual Agency FRT Use Data" form.
- Include **all data elements** in the **order specified** by the above guidelines. (See current version of the Excel Template for proper layout).
- All files must include a header row with column labels. Query data must start on Row 2.
- Please submit **one file** per agency per year; do not submit multiple files for individual users.
- Do **NOT** attach a **pdf** or **scanned** copy of your agency's query data.
- **DCJS may follow-up with your agency regarding any data elements that appear invalid or incomplete. Your submission process is not concluded until all follow-up items are resolved.**

Reporting "No Queries" (Zero Report)

If your agency submitted a Notice of Intent email to the Department of General Services to use Facial Recognition technology but did not perform any queries during the year, please send an email that states '**No Query Data**' to frtdata@dcjs.virginia.gov. This will ensure that your agency is not mistakenly flagged as non-compliant with FRT use data reporting requirements.

Facial Recognition Technology Data Process Diagram



For questions regarding this data collection please contact frtdata@dcjs.virginia.gov.


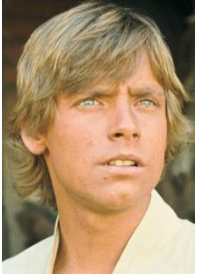
Appendix A: FRT Use Record Structure Example

EXAMPLE CASE NUMBER 123XXX


Below is an example of how searches for a single investigative case could be broken out into 3 separate queries, each requiring a record for FRT use data reporting. Refer to the attached color-coded spreadsheet for a representation of how these queries would be recorded in the actual FRT Use Data Template.

Search = Each instance where a probe image is checked against an image repository



Query = A set of searches performed on the same date for the same subject (regardless of number of searches)

Date of Search	Subject 1 Probe Images	Image Repository Searched	# of Searches	Query ID
12/1/2022		Mugshot System	1	471
		Mugshot System	2	

(Same Date, Same Subject)

Date of Search	Subject 1 Probe Images	Image Repository Searched	# of Searches	Query ID
12/30/2022		DMV Records	1	472
		DMV Records	2	

(Same Subject, Different Date)

Date of Search	Subject 1 Probe Images	Image Repository Searched	# of Searches	Query ID
12/1/2022		DMV Records	1	473
		Mugshot System	2	
		DMV Records	3	
		Mugshot System	4	

(Different Subject, Same Date)

Appendix A: FRT Use Data Record Example

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
	Record ID	Query Date	Number of Searches	Host Agency ORI	Test Case	Host Case Number	Subject ID	User ID	Other Agencies Shared	Requestor ORI	Requestor Case Number	Authorized Use	Criminal Offense Type	Gang/Riot	Nature of Repository	Subject Race	Subject Ethnicity	Subject Gender	List of Candidates	Examiner Offered Lead	Case Closed Involving Lead	
1	471	12/1/2022	2	VAVSP0100	No	123XXX	Suspect1	J03	N	No	N/A	1	Larceny	No	Mug-shot images	W	N	F	N	N	N	
2	472	12/30/2022	2	VAVSP0100	No	123XXX	Suspect1	J03	Yes (Harrisonburg Police Dept.)	VA1120000	205XXX	1	Larceny	No	Driver's license/Other State Identification photographs	W	N	F	Y	Y	U	
3	473	12/1/2022	4	VAVSP0100	No	123XXX	Suspect2	J03	N	No	N/A	1	Larceny	No	Mug-shot images, Driver's license/Other State Identification photographs	U	U	M	Y	N	N	
4																						
5																						
6																						
7																						
8	Color-coded columns correspond to the items shown in the Appendix A example diagrams. Columns in																					
9	standard black font are filled in with valid responses made up for the sake of to completing each																					
10	record.																					
11																						
12																						
13																						