

Detroit Public Safety Headquarters 1301 Third Street, Suite 75-751 Detroit, Michigan 48226

Phone 313•596•1800 Fax 313•596•6818

April 3, 2024

Mr. QuanTez Pressley, Chairperson Board of Police Commissioners Detroit Public Safety Headquarters 1301 Third Street, Suite 7S-767 Detroit, Michigan 48226

Re: POLICIES FOR REVIEW

Dear Chairperson Pressley:

I am pleased to present to you the attached Facial Recognition Policy, new templates for Facial Recognition, and Eyewitness Identification and Lineups Policy that was collaboratively worked on and agreed upon with Philip Mayor, Ramis Wadood, Dan Korobkin, and Nate Wessler of the American Civil Liberties Union (ACLU), Michael Steinberg of the University of Michigan Law School, and the assistance of the United States District Court – Eastern Michigan District.

Should you have any questions, please feel free to contact 2<sup>nd</sup> Deputy Chief Grant Ha, Legal Advisor to the Chief of Police, Monday through Friday, 8:00 a.m. until 4:00 pm at 313-596-1803.

Sincerely,

JAMES E. WHITE Chief of Police

JEW/gh

#### Attachment:

- 1. Facial Recognition Policy
- 2. Facial Recognition Templates
- 3. Eyewitness Identification and Lineups Policy





MANUAI

Series	Effective Date	<b>Review Date</b>	Directive Number		
300 Support		Annually			
Services		-	307.5		
Chapter					
307 - Information Syst	em				
Reviewing Office					
Crime Intelligence			New Directive		
References:			Revised		

### **FACIAL RECOGNITION**

### 307.5 - 1 PURPOSE

The purpose of this policy is to establish acceptable use of Facial Recognition technology by the Detroit Police Department (DPD). Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing investigation of a Part 1 Violent Crime or a first-degree Home Invasion. If an investigative lead is developed through DPD's Facial Recognition program, it shall be considered only an investigative lead that shall not be the sole ground for arrest or to apply for an arrest warrant.

### **307.5 - 2 Definitions**

### 307.5 - 2.1 Biometric Data

Data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and Facial Recognition data.

### 307.5 - 2.2 Examiner

An individual who has received advanced training in the Facial Recognition program and its features. Examiners have at least a working knowledge of the limitations of Facial Recognition. Examiners are qualified to assess image quality and appropriateness for Facial Recognition searches and to perform one-to-many and one-to-one facial image comparisons.

### 307.5 - 2.3 Facial Recognition (FR)

The automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity. All Facial Recognition searches must be corroborated by at least two examiners and one supervisor.

#### **307.5 Facial Recognition**

### 307.5 - 2.4 First-degree Home Invasion

A person who breaks and enters a dwelling with intent to commit a felony, larceny, or assault in the dwelling, a person who enters a dwelling without permission with intent to commit a felony, larceny, or assault in the dwelling, or a person who breaks and enters a dwelling or enters a dwelling without permission and, at any time while he or she is entering, present in, or exiting the dwelling, commits a felony, larceny, or assault is guilty of home invasion in the first degree if at any time while the person is entering, present in, or exiting the dwelling either of the following circumstances exists:

- (a) The person is armed with a dangerous weapon.
- (b) Another person is lawfully present in the dwelling. (MCL 750.110a(2)).

#### 307.5 - 2.5 Part 1 Violent Crimes

For the purposes of this directive, Part 1 Violent Crimes are defined as robbery, sexual assault, aggravated assault, or homicide.

## 307.5 - 2.6 Predictive Analysis

The process of using data to forecast future outcomes.

### 307.5 - 2.7 Reasonable Suspicion

The specific facts and reasonable inferences drawn from those facts to convince an ordinarily prudent person that criminality is at hand.

# 307.5 - 2.8 Statewide Network of Agency Photos (SNAP)

A computer application managed by the SNAP Unit, deployed through the MiCJIN portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

## 307.5 - 3 Prohibited Uses

#### 307.5 - 3.1 Surveillance

Members shall not use Facial Recognition to surveil the public through any camera or video device.

# 307.5 - 3.2 Live Streaming or Recorded Videos

Members shall not use Facial Recognition on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source.

### 307.5 - 3.3 Mobile Facial Recognition

Members shall not use mobile Facial Recognition.

## 307.5 - 3.4 Predictive Analysis

Members shall not use Facial Recognition for predictive analysis.

MANUAL

#### 307.5 Facial Recognition

### 307.5 - 3.5 First Amendment Events

The Detroit Police Department will not violate First, Fourth, and Fourteenth Amendments and will not perform or request Facial Recognition searches about individuals or organizations based solely on the following:

- a. Their religious, political, or social views or activities;
- b. Their participation in a particular noncriminal organization or lawful event; or
- c. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

# 307.5 - 3.6 Facial Recognition Use for Immigration Enforcement

DPD members are strictly prohibited from using Facial Recognition to assess immigration status.

# 307.5 - 4 **Discipline**

- 1. Any violations to this policy shall be deemed major misconduct. Any misuse of the Facial Recognition program will be investigated and reviewed for criminality. The remedy for this misconduct is dismissal from DPD.
- 2. If Facial Recognition is used contrary to section 307.5 -3.5 First Amendment Events, DPD shall notify the Board of Policy Commissioners, the Mayor of Detroit, City Council President, and City Council President Pro Tem within 24 hours of the violation.

# 307.5 - 5 Use of Facial Recognition Technology

## 307.5 - 5.1 Use Limited to Still Images

Facial Recognition technology may only be used on a still image of an individual, including still images captured from video.

# 307.5 - 5.2 Criminal Investigation Required

Members shall not use Facial Recognition technology unless there is reasonable suspicion that use of Facial Recognition technology will provide information relevant to an active or ongoing investigation of a Part 1 Violent Crime or a first-degree Home Invasion.

307.5 - 5.3 An Arrest or Arrest Warrant Request Following Use of Facial Recognition Technology Must Be Supported by Additional Independent Reliable Evidence

Probable cause must be established for an arrest or for an arrest warrant request must be established using legally authorized methods other than Facial Recognition. Examples of other investigative methods may include, but are not limited to cellular data analysis; eyewitness testimony, establishment of a timeline, DNA, etc. A request for an arrest warrant, or an arrest, shall not be made solely on the basis of an investigative lead developed through Facial Recognition technology in combination with a lineup identification. A request for an arrest warrant, or an arrest, must be supported by additional independent reliable evidence.

#### 307.5 Facial Recognition

# 307.5 - 5.4 Process for Requesting Facial Recognition

- 1. Requests for Facial Recognition services shall be submitted to the Crime Intelligence Unit (CIU), with photograph(s) to be reviewed, the incident number, the crime type, and other pertinent information.
- a. Members requesting Facial Recognition services shall affirm that they have completed investigative Facial Recognition training;
- b. Members performing Facial Recognition services shall confirm that the requesting member has made the affirmation above.

# 307.5 - 5.5 Process for Performing Facial Recognition

- 1. Prior to the use of Facial Recognition, a CIU examiner shall complete the Real Time Crime Center Facial Recognition Vetting form, which shall contain:
- a. The requestor's name, rank, and command;
- b. Confirmation that the requestor has affirmed that they have completed investigative Facial Recognition training;
- c. The crime being investigated (Part 1 Violent Crime or first-degree Home Invasion);
- d. The role the individual in the probe image is reasonably suspected to have played in the incident; and
- e. A description of the probe image quality.
- 2. CIU shall reject a request for Facial Recognition when:
  - a. The request fails to identify the requestor's name, rank or command;
  - b. The requestor fails to affirm that they have completed investigative Facial Recognition training;
  - c. The crime being investigated is not a Part 1 Violent Crime or first-degree Home Invasion;
  - d. There is not a reasonable suspicion that the individual in the probe image had a role in the commission of the crime; or
  - e. The quality of the probe image is unsuitable for Facial Recognition.
- 3. CIU shall perform Facial Recognition searches utilizing SNAP, which includes criminal mug shot images. In the event additional analysis is needed for confirmation of an investigative lead, a formal request may be made to MSP to search the state's database. Any such request must be approved by a CIU supervisor.
- 4. If the examiner develops an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor. Both examiners and the CIU supervisor shall sign off on the investigative lead.
- 5. Upon final approval, CIU shall complete an investigative lead report for the requestor. This investigative lead report must be attached to any request for a warrant for any person named in the investigative lead report. The investigative lead report shall include the following language:

MANUAL

### **307.5 Facial Recognition**

- "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources."
- "Facial Recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the probe image's quality, lighting, face angle, and face obstructions, among other factors."
- "Facial Recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

In addition, the investigative lead or vetting report shall also.

- Disclose the probe image used to run the Facial Recognition search (in both its original form and with any enhancements), and identify all features of the probe image that may reduce the reliability of the Facial Recognition result (such as low light, low pixel density, angle of face, partial occlusion of face, etc.), and any enhancements or modifications made to the probe image during the course of the search process;
- Disclose each of the following: the date the investigative lead image was taken, how many other images of the same individual in the investigative lead image exist in the database that was searched, and, if other images of the same individual exist in the database, the dates when each was taken.
- 6. In any case in which charges are filed and in which Facial Recognition technology was used at any stage of the investigation, the member responsible for that investigation shall provide the following to the Wayne County Prosecutor's Office (WCPO):
  - Any investigative lead report and vetting report;
- 7. In the event that an investigative lead cannot be developed, the requestor will be notified that no investigative lead was developed.

#### 307.5 Facial Recognition

## 307.5-5.6 Outside Agency Using Facial Recognition

An outside agency, or investigators from an outside agency, may request *Facial Recognition* searches *by DPD* to assist with investigations only if the following requirements are met:

- Prior to making the request, the outside agency has a formalized agreement (e.g. a memorandum of understanding or an interagency agreement) between DPD and the outside agency;
- b. The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:
  - "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources."
- c. If any agency is found not in compliance with this Directive, *DPD* shall immediately suspend all Facial Recognition requests until the requesting agency becomes in compliance with this Directive.

# 307.5 - 6 Governance and Oversight

## 307.5 - 6.1 LASO & CIU Responsibilities

- 1. The primary responsibility for the operation of *DPD*'s criminal justice information systems, Facial Recognition program and system, operations, and the coordination of personnel, the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Local Agency Security Officer (LASO) who is assigned to Technical Services.
- 2. The LASO will be responsible for the following:
  - a. Overseeing and administering the Facial Recognition program to ensure compliance with applicable laws, regulations, standards, and policy;
  - b. Acting as the authorizing official for individual access to Facial Recognition information;
  - c. Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status; and
  - d. Ensuring that random evaluations of user compliance with system requirements along with this policy and applicable laws are conducted and documented;

MANUAL

#### 307.5 Facial Recognition

- 3. The commanding officer of CIU will be responsible for the following:
  - a. Reviewing Facial Recognition search requests, reviewing the results of Facial Recognition searches, and returning the most likely candidates or candidate images if any, to the requestor.
  - b. Ensuring and documenting that personnel (including investigators from external agencies who request Facial Recognition searches) meet all prerequisites stated in this policy prior to being authorized to use the Facial Recognition system.
- 4. Members of investigative entities shall be responsible for the following:
  - a. In the event that the Facial Recognition program develops an investigative lead, prior to making any probable cause arrest, or requesting a warrant from the (WCPO), the member must obtain written approval from their commanding officer and the commanding officer of Investigative Operations.
- 5. *DPD* is guided by applicable laws, regulations, and standards to ensure that privacy, civil rights, and civil liberties are not violated by this Facial Recognition policy or by the *DPD*'s Facial Recognition information collection, receipt, access, use, dissemination, retention, and procedure.

# 307.5 - 6.2 Weekly Report to the Board of Police Commissioners

DPD shall provide a weekly report to the Board of Police Commissioners with information pertaining to the number of Facial Recognition requests that were fulfilled, the crimes that the Facial Recognition requests were attempting to solve, the number of leads developed from the Facial Recognition program, and the number of searches that did not produce investigative leads. During this report, if there are any upgrades to the Facial Recognition software, any planned changes to the contract, and/or any confirmed policy violations, DPD shall notify the Board of Police Commissioners.

# 307.5 - 6.3 Annual Report to the Board of Police Commissioners

DPD shall provide an annual report to the Board of Police Commissioners. This annual report shall include a summary of the weekly reports and an evaluation of the efficacy of the DPD's Facial Recognition technology. The evaluation shall include any relevant lawsuits or settlements involving Facial Recognition, the number of cases *in which* use of the technology assisted in investigations, and any other relevant factors. This shall be disseminated at the Board of Police Commissioners' meeting, and electronic copy shall be provided to the Board for dissemination to the public.

MANUAL

### **307.5 Facial Recognition**

**307.5 - 6.4** All Policy Changes to the Board of Police Commissioners

DPD shall seek the Board of Police Commissioners' approval regarding any and all changes to this manual directive.

# 307.5 - 7 Security and Maintenance

1. DPD will comply with generally accepted industry or other applicable standards for security to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related DPD activity. DPD's Facial Recognition system will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system.

Access to the *DPD*'s Facial Recognition information from outside the facility will be allowed only over secure networks. All results produced by *DPD* as a result of a Facial Recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee. When such non-electronic dissemination is made, the member shall memorialize the dissemination as follows:

- a. To whom it was released;
- b. Date and time it was released; and
- c. Manner in which it was released (i.e. if by phone, include the number; if in person, include name of witness who saw itreleased).
- All members with access to *DPD*'s information or information systems will report a suspected or confirmed breach to their immediate supervisor who will ensure that the LASO) is notified as soon as possible without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, *or* electric. Following assessment of the suspected or confirmed breach and as soon as practicable, *DPD* will notify the originating agency from which the entity received *F*acial *R*ecognition information of the nature and scope of a suspected or confirmed breach of such information. *DPD* will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.
- 3. All Facial Recognition equipment and Facial Recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

MANUAL

### 307.5 Facial Recognition

- 4. *DPD* will store Facial Recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by members authorized to take such actions.
- 5. Authorized access to the *DPD*'s Facial Recognition system will be granted only to members whose positions and job duties require such access and who have successfully completed a background check and required training.
- 6. Usernames and passwords to the Facial Recognition system are not transferrable, must not be shared by *DPD* members, and must be kept confidential.
- 7. The system administrator (LASO) will ensure that all manufacturer- generated default passwords are replaced with secure passwords before web-based interfacial of the system become operational. User passwords must meet the standards outlined in Manual Directive 307.4, Criminal Justice Information Systems (CJIS).
- 8. Queries made to *DPD*'s Facial Recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
- 9. DPD will maintain an audit trail of requested, accessed, searched, or disseminated Facial Recognition information. An audit trail will be kept for a minimum of one (1) year of requests, access, and searches of Facial Recognition information for specific purposes and of what Facial Recognition information is disseminated to each individual in response to the request. Audit logs will include:
  - a. The name and unit of the law enforcement user;
  - b. The date of access:
  - c. Case number; and
  - d. The authorized law enforcement or public safety justification for access including a relevant case number.

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources.

Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors.

Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

## REAL TIME CRIME CENTER — FACIAL RECOGNITION INVESTIGATIVE LEAD

Page 2 of 3

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and **1S NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT.** Any possible connection or involvement of any subject to the investigation must be determined through further Independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST #:	23-00						
REQUEST DATE/TIME:							
REPORT NUMBER:							
CRIME:	☐ Homicide ☑ Robbery/Carjacking ☐ Aggravated Assault/NFS ☐ CSC 1/CSC 3 ☐ Home Invasion 1						
REQUESTER NAME:			RANK:	Choo	se an item	COMMAND:	
REASON:	Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion  Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)						
	CALLED TO F	BOTTH WE		PARE	Mauri	Te-Diffa	
IMAGES:	ORIGINAL IMAGE		INQUIRY IMAGE		INVESTIGATIVE LEAD		
IMAGE SOURCE:	Choose an item		Choose an item.		SNAP	Date	
IMAGE ENHANCEMENTS:	Choose	an item	Ch	oose ai	ritem.	r	lone
# OF IMAGES PRODUCED IN GALLERY:		# OF LEAD IMAGES IN DATABASE:		1	DATES OF LEAD MAGES:		
	B REST	CONTRACTOR OF	DE I	CAN.		A COLUMN	
NAME:							
ALIAS:							
DOB:							
DL/PID #:							
SID #:	FBI #:						
ADDRESS:							
SOCIAL MEDIA:							V
INCARCERATION STATUS:	Choose an item. <b>SOURCE</b>		: (	Choose an item		E:	
INVESTIGATIVE LEAD PROCESS:	<ul> <li>         ⊠ Statewide Network of Agency Photos (SNAP)     </li> <li>         □ DataWorks Plus     </li> <li>         □ Forwarded to Michigan State Police (MSP) for additional assistance     </li> </ul>						
er fix ofter fit		SELVER LINE	LYTT		4 1 1 1	art lan	Partition in
DATE/TIME FINALIZED:							
CIU PERSONNEL:							
CIU PEER REVIEWER:							
SUPERVISOR:							

# REAL TIME CRIME CENTER — FACIAL RECOGNITION INVESTIGATIVE LEAD

Page 3 of 3

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

FURTHER INVESTIGATION WAS COMPLETED TO DETERMINE THE NECESSARY PROBABLE OF	CAUSE TO PROCEED
WITH AN ARREST OF THE INDIVIDUAL AND/OR SUBMISSION OF A WARRANT:	
□ CODIS Match	
☐ AFIS hit	
☐ CDR warrant results	
☐ PEN warrant results	
☐ Social Media warrant results	
☐ Witness Statements	
☐ Other:	
□ Other:	
☐ Other:	
INVESTIGATIVE OPERATIONS:	
Prior to an arrest of an individual and/or submission of a warrant, the information was revi	iewed and:
□ APPROVED	
□ DENIED	
Investigate Operations Captain (print):	
Signature: Date:	717
COMMANDING OFFICER:	
Prior to an arrest of an individual and/or submission of a warrant, the information was revi	ewed and:
☐ APPROVED	
□ DENIED	
Commanding Officer (print):	
Signature: Date:	

# REAL TIME CRIME CENTER — FACIAL RECOGNITION VETTING

Page 1 of 1

The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further independent investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fall to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST DATE/TIME:						
REPORT NUMBER:						
CRIME:	□Homicide □Robb	ery/Carjacking 🗆 Ag	gravated Assaul	t/NFS ⊠CS	C 1/CSC 3 □Hom	e Invasion 1
REQUESTER NAME:		RANK:	Choose		COMMAND:	
IMAGE SOURCE:				1	R OF IMAGES:	
REASON:	Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion  Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)					
					175-1715-153	
	PER POLICE RE	PORT, SUPPLEMEN	NTS, AND DET	ECTIVE NO	TES:	
PROBE ROLE IN CRIME:	Choose an item					
SUSPECT KNOWN:	Choose an item.					
				Wind W	TALL NAME:	
		РНОТО QU	ALITY:			
FILE SIZE:			DIMEN	SIONS:		
RACE:			SEX:		-	
FACIAL OBSTRUCTIONS:						
FACE ORIENTATION:						
IMAGE BRIGHTNESS:				-		
TATTOOS/FACIAL PIERCINGS/BIRTH MARKS:						
NUMBER OF USABLE IMAGES:						
	San American	North Alakes	STATES.		A. Cor	Tax of the State
STATUS OF REQUEST:	Choose an item	6				
IF REJECTED, WHY?						
		Charles on the				T
ANALYST:			DA	TE/TIME:		
REVIEWER:			DA	TE/TIME:		
SUPERVISOR:			DA	TE/TIME:		
			-			

Intel Number: 23-