



**LAW ENFORCEMENT INFORMATION EXCHANGE**

**NCR-LINX FACIAL RECOGNITION**

**PILOT PROJECT**

**CRIMINAL JUSTICE INFORMATION NETWORK**

**GOVERNING BOARD MEETING**

**MARCH 26, 2019**

**CATHERINE MILLER**



# NCR-LINX FACIAL RECOGNITION

- Facial Recognition Investigative Lead System (FRILS)
  - Phase 1 Pilot Project Re-Cap
- Stand Alone System housed at Fairfax County Police
- MOU and Policy Documents
- User Agreement
  - LinX Users Only
  - FR Training

**National Capital Region  
Facial Recognition Investigative Lead System  
User Policy Agreement**

The National Capital Region (NCR) Facial Recognition Investigative Lead System Pilot Project is a part of the NCR-Biometric and NCR-Linx programs. The pilot project's complete timeline will be one year starting after Board approval and data load.

The purpose of the pilot project is further the evaluation of a facial recognition application for the NCR utilizing only arrest and booking photos from the NCR-Linx system. This pilot project is intended to further law enforcement or criminal investigations by providing potential investigative leads of unknown suspects based on high quality surveillance photos. All requirements for the reviewing and handling of NCR-Linx data extended to the facial recognition data. For the pilot project all facial recognition examiners will be NCR-Linx trained and certified users.

In addition to the restrictions imposed by NCR-Linx and NDEX, examiners and others involved in the facial recognition pilot agree to the following provisions:

- All information relevant to the pilot project will be considered highly confidential. Dissemination of information outside the pilot project testing group and governance board is not permitted except as published in the Final Report on the project.
  - Any potential investigative leads of suspects will be reported back to the detective submitting the probe image.
  - It is also important to ensure that any cases going to court will need to obtain the original photo from the contributing agency as photos in this system and in LinX are just a duplicate copy of the original owned by the contributing agency.
- Any user suspended or revoked from the NCR-Linx system will also be suspended or revoked from the facial recognition pilot project.
- Hardware use of the facial recognition software will be facilitated over a secure internet connection.
- Provide best effort to attend, either in person or via teleconference, meetings associated with the pilot project.
- Be a LinX trained user or attend LinX training prior to participating in this pilot.
  - In all cases a user credential on the NCR-Linx system will be a valid user of a law enforcement agency. Each pilot user will have been trained on LinX and will have signed the appropriate LinX user Security Agreement.
- Attend the required facial recognition software training.
- Bring in cases, SOGUs, and watch lists from participating agency to include in the test.

8. Follow all existing NCR-Linx policies and procedures for all users

9. Provide opinions and report experiences with regard to the test pilot. A form will be provided to complete with each test.

10. Review and provide feedback on final pilot project reports.

Please complete the below information, sign and return this policy

Name: \_\_\_\_\_

Supervisor: \_\_\_\_\_ Date: \_\_\_\_\_

Agency: \_\_\_\_\_


LinX User ID: \_\_\_\_\_

email address: \_\_\_\_\_

Telephone number: \_\_\_\_\_

Signed: \_\_\_\_\_ Date: \_\_\_\_\_


Supervisor Signature: \_\_\_\_\_ Date: \_\_\_\_\_



**Face Recognition  
Policy Development Template**

For Use in Criminal Intelligence  
and Investigative Activities

December 2017



# NCR-LINX FR TEST PILOT - SUCCESS STORY

## *Smart Phone Digital Photo Comparison Exonerates Suspect*

- *A witness in a gang-related assault case provided smartphone photos of the suspects to the detective working the case. One of the photos of a suspect was able to be run using facial recognition software and an investigative lead was developed. Upon further investigation confirmation of the suspect's name was made and during the investigation it was found that the suspect was in jail in another location at the time of the crime. Verification of the suspect was made based on the photo of him and the tattoos on his arm. Apparently, the witness provided an incorrect photo of one of the suspects and the facial recognition system, along with further investigation, saved investigators time, and more importantly, saved the individual from being arrested for a case in which he was not involved.*

# NCR-LINX FACIAL RECOGNITION

## ➤ Training conducted (Phase 1 & Phase 2)

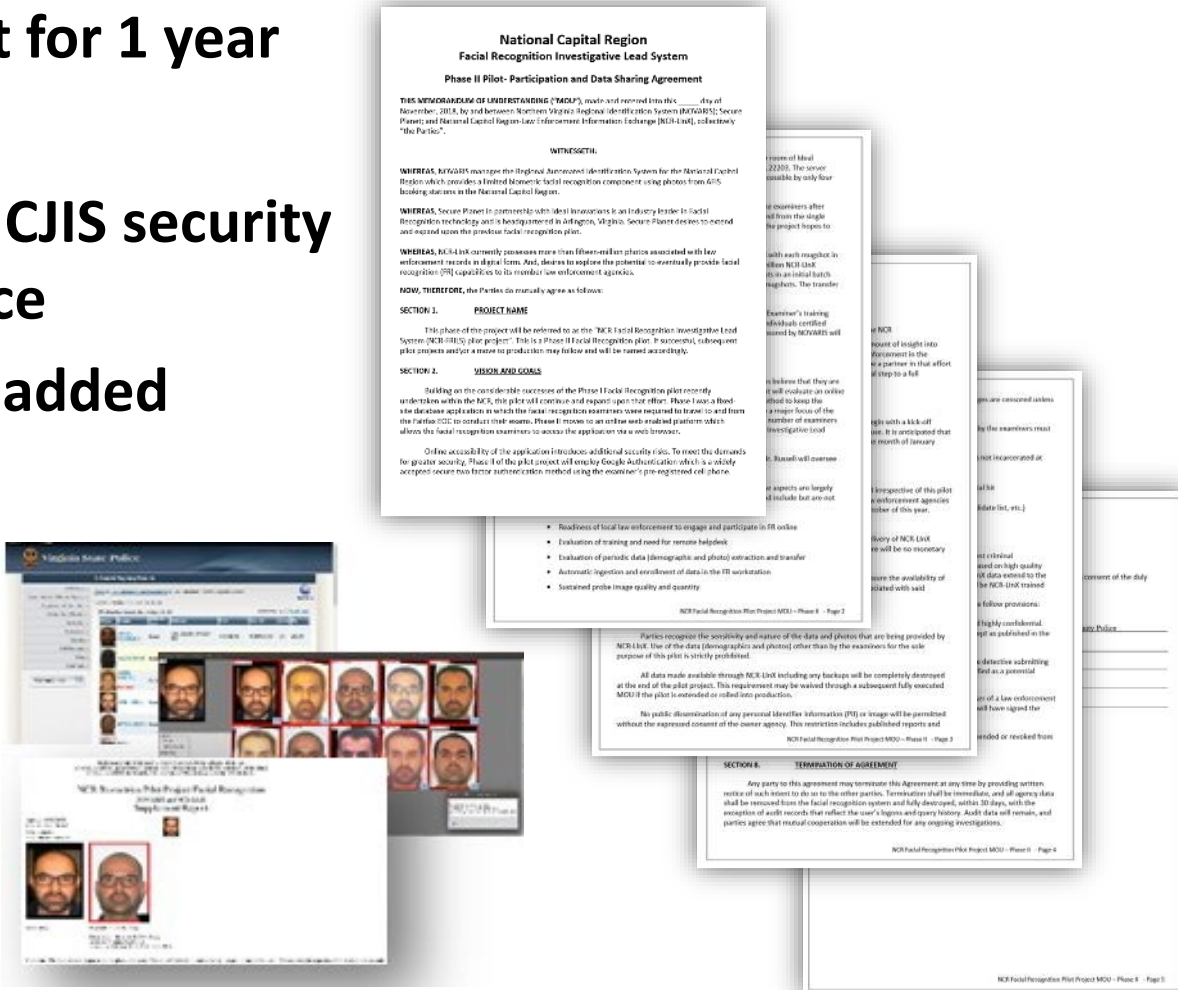
– Agencies with Users Trained between late 2016 and Nov 2018

- Fairfax County Police
- Fairfax City Police
- DC Metropolitan Police
- Alexandria Police
- Prince William County PD
- MD National Capital Park PD
- WMATA
- ATF
- Montgomery County Police
- Loudoun County SO
- Prince George's County PD
- Arlington County PD
- Baltimore City PD



# NCR-LINX FACIAL RECOGNITION

- Phase 2 Pilot Project for 1 year
- Cloud based
- Hosted system with CJIS security requirements in place
- Additional Features added
  - Reduce duplicates
  - Video analysis
  - Increased speed
  - Profile matching
- Expanded Policy & MOU Documents



**National Capital Region  
Facial Recognition Investigative Lead System  
Phase II Pilot- Participation and Data Sharing Agreement**

**WITNESSETH:**

WHEREAS, NAVFORS manages the Regional Automated Identification System for the National Capital Region which includes a hybrid biometric facial recognition component using photos from DHS briefing centers in the National Capital Region;

WHEREAS, Secure Power in partnership with Intel Innovation is an industry leader in facial recognition technology and is being awarded in Arlington, Virginia, Secure Power desires to extend and expand upon the previous facial recognition pilot;

WHEREAS, NCR-LINX currently processes more than eleven-million photos associated with law enforcement records in digital form. And, desires to explore the potential to eventually provide facial recognition (FR) capabilities to its member law enforcement agencies;

NOW, THEREFORE, the Parties do mutually agree as follows:

**SECTION 1. PROJECT NAME**

This phase of the project will be referred to as the "NCR Facial Recognition Investigative Lead System (NCR-FRIS) pilot project". This is a Phase II facial recognition pilot. If successful, subsequent pilot projects and/or a move to production may follow and will be named accordingly.

**SECTION 2. VISION AND GOALS**

Building on the considerable successes of the Phase I facial recognition pilot recently undertaken within the NCR, this pilot will continue and expand upon that effort. There have been a number of lessons learned in which the facial recognition system was required to know to and from the NCR-FRIS to conduct their work. Phase II moves to an online web-enabled platform which allows the facial recognition examiners to access the application via a web browser.

On the accessibility of the application introduce additional security (i.e., to meet the demands for greater security, Phase II of the pilot project will employ Google Authentication which is a widely accepted secure two factor authentication method using the examiner's pre-registered cell phone.

- Readiness of local law enforcement to engage and participate in FR online
- Evaluation of training and need for remote helpdesk
- Evaluation of periodic data (demographics and photo) extraction and transfer
- Automatic ingestion and enrollment of data in the FR workstation
- Sustained probe image quality and quantity

**SECTION 8. TERMINATION OF AGREEMENT**

Any party to this agreement may terminate this Agreement at any time by providing written notice of such intent to the other parties. Termination shall be immediate, and all agency data shall be removed from the facial recognition system and fully destroyed, within 30 days, with the exception of audit records that reflect the user's logins and query history. Audit data will remain, and parties agree that mutual cooperation will be extended for any ongoing investigations.

# LAW ENFORCEMENT IMAGING TECHNOLOGY TASK FORCE (LEITTF)

- **IACP and IJIS Institute Combined Task Force**
  - Meets Monthly and at IACP and IACP LEIT Conferences
- **Scope and Goals**
  - Present Issues and Recommendations Regarding General Law Enforcement Use of Facial Recognition Systems (FRS)
  - Inform & Guide Law Enforcement Leaders about FRS
  - Provide Use Cases with Success Stories
  - Ensure FRS Technology Providers have Congruent Knowledge and Intentions
  - Avoid duplicative efforts/scan existing FRS initiatives
  - Help LE Community Create/Influence Policy & Legislation
- **Outcome**
  - Detailed Document consisting of Use Cases and Success Stories for Facial Recognition to also include a Legislative Component
  - Goal is to Finalize and publish in January

# IACP / IJIS IMAGING TASK FORCE

- The Law Enforcement Imaging Technology Task Force (LEITTF) created a catalog of facial recognition use cases for criminal justice agencies, which includes uses by police officers, sheriff's deputies, investigators, and supporting personnel wherever they exist.
- The examination of uses covers typical settings where law enforcement interacts with persons such as large venues, transportation hubs, correctional facilities, motor vehicle stops, crime scenes, and other everyday situations.
- The intention is to briefly describe facial recognition systems and their parameters, determine ways in which facial recognition is being used, and to document cases which demonstrate the technology's ability to protect the public.
- The objective is to empower public safety practitioners and industry innovators to communicate the ability of facial recognition to policy makers and the public, while reducing misunderstanding and minimizing the potential misuse. *(Click the picture to take you to the Report)*

