EXECUTIVE SUMMARY

The Digital Mugshot System (D.M.S.) is the Peel Regional Police (PRP) centralized known offender database, which provides a complete arrest record with finger/palm prints, demographics, scars-marks-tattoos and booking images. Despite the evidentiary value of the photo repository within D.M.S., no real-time identification system has been implemented to mine the photos for matches with suspects of unsolved criminal activity.

As a real-time identification system, facial recognition technology is a tool that aims to assist lead investigators identify or authenticate individuals by comparing their facial geometry and generating a morphological map to compare against a database of faces and searching for one or more likely candidate matches. For facial recognition to be successful there needs to be a quality digital image of an individual's face, a database of digital images or identified individuals, and facial recognition software that will accurately find a match between the two.

The Facial Recognition Software (FRS) will be utilized jointly by York Regional Police and Peel Regional Police Forensic Identifications Units. It is the intention for York Regional Police and Peel Regional Police to co-share a pool of respective booking images in the Facial Recognition System (FR System) to gain the efficiencies and advantages of such a share agreement. PRP will be responsible for keeping the FR system up to date with their booking image data and York will share a similar responsibility. The comparison capabilities of the FR system will be exercised against this joint pool of images.

The FRS project aims to modernize the way in which unknown subjects are identified, ultimately enhancing public safety by ensuring those suspected of criminal activity are identified more efficiently and more accurately. The following four objectives summarize the intentions of the FRS project:

1. Increase solved crime rates by enhancing criminal detection methods via the implementation and utilization of Facial Recognition software.

2. Create efficiencies in the identification of potential suspects in a criminal investigation, via decreasing investigator time spent on manually searching data

3. Enhance operational response times in identifications while reducing potential loss of evidence

4. Leverage data through emerging technologies to be more effective in keeping communities safe.

A Privacy Impact Assessment of the proposed Facial Recognition System was initiated and Consultations with the Information and Privacy Commission of Ontario and, on the topic of s. 8 of the *Charter*, the Ministry of the Attorney General – Crown Law Office Criminal took place as part of implementation of this project.

The Privacy Impact Assessment will be reviewed and updated as the FRS project goes live and in line with the evolving legal framework guiding the use of Facial Recognition Technology.

SUMMARY OF RECOMMENDATIONS

2.1 Notice

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
There should be community engagement with the public prior to the go live date. Ensure that a media release is posted on the PRP external website to notify the public of PRP's use of facial recognition software. This will also demonstrate PRP's commitment to transparency.	Yes	

2.2 Contact Information

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
Ensure that the PRP website is updated to provide the D/Sgt. of Forensic Identification Unit and the FOI Unit contact information to the public should they have any concerns regarding the use of FR or any privacy concerns	Yes	PRP website will be updated prior to Go Live date.

2.3 Limitation on Use of FR System

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
Ensure that the limitations of use of the FR system are incorporated into the training of the FR analysts.	Yes, all staff using the FRS have completed training which incorporated the policies and procedures on the use of the FRS.	N/A
Ensure that prior to uploading the probe images to FR system that the comparison requested is for the purposes outlined in the MOU and Directive	The FR analyst will review all requests to ensure they meet the requirements outlined in the FR procedure prior to uploading the	N/A

	probe image conducting the comparison	
Ensure there are guidelines establish so that all PRP officers understand the limitations of the use of FR and the limitations on the FRS comparisons.	Yes. A procedure will exist governing FR and use of the FR System. In addition, a mandatory CPKN was created (Responsible and Ethical Use of Facial Recognition) for all uniform officers	N/A
Develop a unit process to govern the intake and management of internal and external requests for comparison.	Yes. Part of Directive as well as PRP created an intake process for receiving FRS requests from internal and external agencies.	
Ensure that FR will not be used for real-time use/live streaming.	Yes. Use is governed in the MOU between YRP PRP and in YRP's FR procedure. No real time use. Only "post event"	N/A
Ensure that only legally obtained booking images will be used for the comparisons, no scraping of public media for the database.	Yes. Only booking images from the YRP & PRP mugshot data bases will be used for the comparisons in the FR system	N/A

2.4 Limitations on the collection of Probe Images

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
Ensure that if the image of a suspect or person of interest is from a video recording that may contain images of several persons that only the image of the suspect or person of interest is used for the comparison.	Yes. The requesting officer will have to identify the suspect or person of interest in their request made to the FI Unit prior to the video being uploaded to the FR System	N/A
Ensure that the collection of the probe image was legally obtained “law enforcement purposes only”.	Yes. The requesting officer will have to provide the associated General Occurrence Number on the FR request forwarded to FI. All requests will contain PR Occurrence number	N/A

2.5 Limitations on the retention of Probe images

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
Ensure that once the probe image has been identified that is removed from the FR system.	Yes, included in the FR procedure	N/A
Conduct yearly audits and communicate with OIC’s to determine if criminal investigations are still active or have been concluded to validate the retention of the Probe Image in the Probe Image Data Pool	Yes, included in the FR Procedure. Also, Niche will collect all stats to measure the program success.	N/A

2.6 Updates and Deletions to Booking Images in FR system

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
Ensure that all booking images and metadata retained in the FR system is current and up to date.	Yes. Any updates in the Niche System will be synchronized with a corresponding action in the FR system via a system interface	N/A
Ensure that all booking images and metadata that has been removed or sealed in the Cogent Mugshot System (YRP) or Niche RMS (YRP) has been removed from the FR system.	Yes. Any updates in the Niche RMS will be synchronized with a corresponding action in the FR system via a system interface	N/A

2.7 Procedures

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
Ensure there is an PRP procedure in place to govern the operational use of Facial Recognition Software prior to implementation.	Yes. Procedure for FRS has been created	N/A
Ensure that the MOU between YRP and PRP covers user authorization, security protocols and all key aspects of access and use of the FR system	Yes, covered in MOU between YRP & PRP	N/A

2.8 Security Measures

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
Ensure the FR system is restricted to trained Facial Recognition Analysts with valid agency use.	Yes. Access will be restricted to PRP's Facial Recognition Analysts and	N/A

	designated IT staff.	
Ensure the FR system maintains audit trails and generates reports of all comparisons in the system including date-time, probe images used and search results accessed. Conduct audits to verify compliance.	Yes. FR system maintains audit trails and generates reports (i.e. who did what and when)	
Ensure there are login security measures in place.	Yes. The FRS requires separate user id and passwords for each user. The system can only be accessed when the PRP staff members are on the PRP network or via VPN. PRP has setup an extra security layer using Okta Single Sign On (SSO) mechanism.	

2.9 Training

Recommendation	**Actions completed? (Y/N)**	**If no action taken, risk accepted? (Y/N)**
Ensure the users have undergone the mandatory "Face Comparison and Identification Training".	Yes. Ongoing. Currently 3 civilians and 3 officers have been trained	N/A
Service wide training for all investigators requesting facial recognition as part of their investigation	Yes. CPKN-Ethical and Responsible use of Facial Recognition.	

2.10 Accuracy

Recommendation	Actions completed? (Y/N)	If no action taken, risk accepted? (Y/N)
That FI Unit consider implementation of an FRS policy to govern mandatory thresholds and best practices pertaining to: 1. Similarity Score 2. False acceptance rate 3. False rejection rate.	Yes. The system will setup thresholds based on best practices and FISWG (https://fiswg.org/)	
Conduct necessary testing and evaluation of the technology	Proof of Concept (POC) phase was done as part of the RFP process to make sure software performed well. Ongoing evaluation will take place going forward.	N/A