MEMORANDUM OF UNDERSTANDING

BETWEEN

MIAMI-DADE COUNTY AND

PARTNER LAW ENFORCEMENT AGENCIES

For Sharing LPR Detection Data and Hotlists on Insight LPR's Platform

I. OVERVIEW

A. Introduction:

This Memorandum of Understanding ("MOU") outlines the conditions under which Miami-Dade County ("County"), by and through the Miami-Dade Police Department (MDPD), and partner law enforcement agencies (together, "Partner Agencies") will share and use license plate recognition ("LPR") data ("LPR Data") and/or LPR Data files ("Hotlist") information stored on the Azure Government Cloud ("AGC") and accessed using Insight systems ("Insight LPR System"). The Insight LPR System provides for simple point-and-click data sharing between credentialed Partner Agency administrators with data sharing privileges enabled by their respective agencies, provided the agencies have entered into this MOU. **Sharing of data between Partner Agencies pursuant to this MOU includes the authority to share by, between and among all signatory partner agencies.**

B. Description of LPR Data:

The Insight LPR Data System is a computer-based system that utilizes emerging technology to capture a color image, as well as an infrared image, of the license plate of a vehicle. The infrared image is converted into a text file utilizing optical character recognition ("OCR") technology. The text file is automatically compared against the stored Hotlist, which may contain information on stolen or wanted vehicles as well as vehicles associated with Amber Alerts, warrant subjects, and Party-defined information.

LPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signal poles. LPR Data systems typically include the necessary equipment to scan plates, notify the end user of a vehicle match, and upload the LPR detection data into an LPR repository for retention and research.

The Partner Agencies entering into this MOU are doing so in order to share LPR detection data and/or hotlist information.

C. Term

This MOU will be effective upon signature by all parties, and will expire on January 7, 2025, unless terminated earlier. This MOU may be renewed for two, five-years terms. The MOU may be terminated at any time when a Partner Agency administrator ("Administrator") revokes data sharing access from one or all Partner Agencies.

II. AUTHORIZED RELEASE OF INFORMATION

A. Sharing of Information:

Each Partner Agency authorizes the other to access its LPR Data and/or Hotlist information that resides in the AGC (as permitted by applicable law).

B. Limitation on Information Sharing:

LPR Data and/or Hotlist information shall only be shared with or released to authorized employees of each Party who have an approved login and password ("Authorized Users"), and a need and/or right to know.

III. INFORMATION OWNERSHIP

A. Ownership:

Each Partner Agency retains control of all information in its account. Each Partner Agency is responsible for creating, updating, and deleting records in its own account according to its own retention policies. Each Partner Agency shall use reasonable efforts to ensure the completeness and accuracy of its data.

B. Release of Information:

Partner Agencies and Authorized Users shall release or make available information accessed from an LPR account only to persons or entities authorized to receive LPR information. **Subject to Section III(D) below, no Partner Agency shall release or make available information contained in its LPR account to a non-Partner Agency.**

C. Unauthorized Requests:

If a Partner Agency receives a request for information in an LPR account by anyone who is not authorized to receive information from the LPR account, that Partner Agency shall refer the request to the law enforcement agency that originated the requested information ("Source Agency").

D. Public Record Requests, Subpoenas and Court Orders:

Any Partner Agency receiving a public records request, subpoena, or court order ("Legal Request") for information in an LPR account not authored by or originated by that Partner Agency shall immediately provide a copy of the Legal Request to the Source Agency, prior to providing a response to the Legal Request.

IV. USER ACCESS

A. Login Application Process:

Each Partner Agency's Administrator is responsible for management of user accounts at that Partner Agency. Each Partner Agency agrees that all authorized users shall be limited to current employees who are legally authorized to review criminal history data for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the

Administrator. The Administrator shall have discretion to deny or revoke individual access for their respective agency.

B. Login Assignment:

Each Authorized User will be issued a user login and a password by the Partner Agency's Administrator. Authorized Users may be assigned to groups that have different levels of access rights based on the level of restriction of the information.

C. Termination of Logins:

Each Partner Agency's Administrator is responsible for timely removal of any login accounts as Authorized Users leave the Partner Agency, no longer qualify for access into the system, or are denied access by the Administrator for any other reason.

D. Intended Use:

Each Authorized User agrees that LPR Data, hotlist information, and the networking resources are to be used solely for law enforcement purposes only and consistent with the law, including (but not limited to) requirements of the Criminal Justice Information Services Division of the FBI. Authorized Users shall not use or share the information for any unethical, illegal, criminal, or commercial purpose.

E. Limitations on Use of Logins:

An Authorized User shall not access information in an LPR repository by using a name or password that was assigned to another user. An Authorized User shall not give his or her password to another person, including another user, to access the system.

F. Audit Trail:

Each transaction is to be logged in such a way as to create a reviewable audit trail. Each Administrator shall conduct an internal audit on a periodic basis to ensure user queries are made for legitimate law enforcement purposes only. This information shall be recorded and retained to allow the Administrator to complete the internal audit. Each Administrator shall maintain the audit trail pursuant to the retention policies of that Partner Agency. Requests for transaction logs shall be made in writing to the Administrator, who shall provide the logs to the requesting party within a reasonable amount of time.

V. INDEMNIFICATION

Each party to this MOU agrees to assume responsibility for the acts, omissions, or conduct of such party's own employees while participating herein and pursuant to this MOU, subject to the provisions of section 768.28, Florida Statutes, where applicable. "Assume Responsibility" shall mean incurring and any all costs associated with any suit, action, or claim for damages arising from the performance of this MOU.

VI. CONFIDENTIALITY OF INFORMATION

A. Information Confidentiality:

Information in an LPR account is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information in an LPR account. Otherwise, the information shall be kept confidential for purposes of not compromising active investigations or undercover operations, jeopardizing officer, or public safety.

B. Internal Requests for Information:

An Authorized User who receives a request from a non-authorized requestor for information in an LPR account shall not release that information but may refer the requestor to the Source Agency.

C. Removal or Editing of Records:

Partner Agencies shall determine their own schedule for record deletion and other edits to their own data. This will be determined by policy and/or legal requirements.

Each Partner Agency acknowledges that it has received a copy of this MOU and will comply with its terms and conditions.

SIGNATURES ON FOLLOWING PAGES

IN WITNESS WHEREOF, the parties have caused this MOU to be executed by their respective and duly authorized officers on the day and year written below.

FOR MIAMI-DADE COUNTY:

_____ _____
Daniella Levine Cava, Mayor Date

_____ _____
Stephanie V. Daniels, Director Date
Miami-Dade Police Department

ATTEST: Juan Fernandez-Barquin
Clerk of the Court and Comptroller

By: _____

Print Name: _____

Date: _____

APPROVED AS TO FORM AND LEGAL SUFFICIENCY

_____ _____
Anita Viciana Zapata Date
Assistant County Attorney
Miami-Dade County, Florida

FOR CITY OF NORTH PORT, FLORIDA:

_____ _____
Alice White, Mayor Date

_____ _____
Todd R. Garrison, Chief Date
North Port Police Department

ATTEST:

_____ _____
Heather Faust, MMC Date
City Clerk
North Port, Florida

APPROVED AS TO FORM AND LEGAL SUFFICIENCY:

_____ _____
Amber L. Slayton, B.C.S. Date
City Attorney
North Port, Florida