



**MEMORANDUM OF UNDERSTANDING (MOU)
MIAMI DADE POLICE DEPARTMENT (MDPD)
AND
PARTICIPATING LAW ENFORCEMENT AGENCY (PLEA)
FOR PHOTO IMAGING (PI) SYSTEM ACCESS**

I. ACCESS PROCESS:

A law enforcement agency wanting access to the PI System will be required to complete the Agency Access Request Form (AARF) prior to this MOU taking effect. No agency will be allowed to participate without complying with the minimum requirements set forth in the AARF.

The AARF is to be completed and signed by the PLEA's Police Chief. This will inform the agency of the necessary and correct network line bandwidth needed, if not currently in place.

The PLEA will be required to appoint a **Technical Liaison or Designee** to act as a contact person responsible for Network Connection to MDPD and all other technical issues. The **Technical Liaison or Designee** will be responsible to report, receive, troubleshoot, and resolve any computer or network related issues with MDPD.

When completed, the AARF should be returned to the current MDPD PI Project Manager, via e-mail. Currently the PI Project Manager can be reached at PI.SUPPORT@mdpd.com.

II. GENERAL PROVISION:

The purpose of this MOU is to establish the terms and conditions for accessing the MDPD computerized PI System.

The PI System and related components consist of booking photographs, along with personal property and related arrest data of arrested individuals (adults/juveniles) that have been processed by the Miami-Dade Corrections and Rehabilitation Department (MDCRD), and the Juvenile Assessment Center (JAC). The booking records are processed in real-time mode and are available in the PI System. The PI System is a web based system allowing law enforcement agencies in Miami-Dade County to have access to the application via the web through secured agency intranet access. The databases currently available are:

- Miami-Dade Adult Arrest Records;
- Miami-Dade Juvenile Arrest Records;
- MDPD Forensic Drawings: Composite, Age Progression, Re-Constructive Face, Postmortem;
- Gang Information;
- Burglary and Auto Theft.

Amendments to the current MOU may be necessary. Specifically, there are future plans to add other databases from different areas of the country, such as the northeastern United States and other Florida locations. These additional databases

will also be made available through the PI System to participating agencies within Miami-Dade County. Consequently, new terms and conditions may be required. The PLEA will be informed of any new terms and conditions. The PLEA will be given the opportunity to review any and all changes and will be given the option of terminating their involvement or continuing their participation.

PLEA will be considered to be part of the Photo Imaging MDPD Enterprise Network and shall be referred to as PLEA.

III. AGREEMENT TERMS AND CONDITIONS:

The PLEA agrees to abide by the terms and conditions set forth in this MOU, specifically, but not limited to, any and all technological requirements, financial responsibilities, personnel requirements, security guidelines, and procedural guidelines. Any security or communication breach will be considered a breach of this agreement and will allow the MDPD in its sole discretion to immediately terminate and/or suspend the participating agencies usage of the PI System and/or that of the violating party.

The following activities are specifically prohibited under this agreement pursuant to MDPD's security policy which could result in MDPD immediately suspending or revoking the user's access or the entire PLEA's right to access the application (PI System).

- Interfering with, tampering with, or disrupting resources of the PI System network or its PLEA;
- Intentionally transmitting any computer viruses, worms, or other malicious software;
- Attempting to access, accessing, or exploiting unauthorized resources;
- Knowingly enabling inappropriate levels of access or exploitation of resources by others;
- Downloading sensitive or confidential electronic information/data to computers that are not adequately configured to protect such information/data from unauthorized access;
- Disclosing any unauthorized electronic information/data;
- Violating Agency, Commonwealth, or federal laws, regulations, policies and/or procedures;
- Failing to cooperate with officials during an investigation of the misuse of the PI System;
- PLEAs are prohibited from electronically sharing any arrest photographs or related arrest data with any non-law enforcement agency or any private entity or individual via network connection or any other access.

IV. HOLD HARMLESS:

All of the materials in these databases are subject to Florida public records laws pursuant to Florida Statutes Chapter 119, Public Records. No agency having access to these records should release any information pursuant to a public records request without first notifying the MDPD Information Technology Services Bureau. This will be done in order to ensure exempt information is not disseminated to the public that may compromise active police investigations, for example.

This information is strictly for law enforcement use and must **not** be shared. If this information is shared, used, or in any way disseminated by any employee of the PLEA,

without the expressed consent of the MDPD, MDPD reserves the right to immediately terminate this agreement without notice.

V. No Rights:

This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable by law or otherwise by any third party against the parties, the State of Florida, Miami-Dade County, or the officers, employees, agents, or other associated personnel thereof.

VI. Liability:

To the extent permitted by law and as limited by §768.28, Florida Statutes, each party shall assume the liability arising from acts taken by its personnel pursuant to this MOU. In no event shall a party be liable for acts, omissions, or conduct of the officers, employees or agents of the other participating party of this MOU and neither party intends a waiver of sovereign immunity or the limits provided by §768.28, Florida Statutes.

VII. CONNECTIVITY REQUIREMENT:

The PLEA is responsible for obtaining and funding a secured high speed connection (DSL, cable, etcetera). In order to establish a network connection to MDPD, the PLEA must connect via any of the following: NetMotion, Secure Socket Layer Virtual Private Network, or a direct Metro-Ethernet line or any other type including DSL which will be paid solely by the PLEA for the initial connection and line charges as well as on a yearly recurring basis. Furthermore, the PLEA will be responsible for all cost associated with the termination of any contract entered into, if the service is no longer needed. If using a Metro-Ethernet Line, the user must have 128 bit encryption on the line by using a VPN. All communications access to the specific applications or systems will be controlled with firewalls and the use of antivirus software. The PLEA may utilize any of the following carriers to secure the connection:

- AT&T Wireless which is currently being used by MDPD;
- Any cellular carrier authorized in the State of Florida; or
- AT&T Business.

Please note that dial-up access via the Internet as an access protocol method will not be accepted due to insufficient performance and security issues.

VIII. SUPPORT:

In the event the PLEA encounters a technical problem(s) using the PI System, the participating agency agrees to provide the first line of support for its users through their ***Technical Liaison or Designee*** first. The PLEA will try to determine where the problem lies and take appropriate action. When the network problem lies inside of the PLEA's demarcation line (network connection to ATT, etcetera) they will be responsible for addressing their own network problem. If the network problem is related to the AFIS (fingerprints) network connection the ***Technical Liaison or Designee*** will contact the MDPD's Shift Commander at 305-596-8176 and request assistance from the on-call MDPD technical support personnel. The ***Technical Liaison or Designee*** will identify the PLEA, provide their contact information, and

report the network connection problem. If the PI System is being non-responsive, please send an email with detailed information to the current MDPD PI System Project Manager at PI.SUPPORT@mdpd.com. If the MDPD network or PI System is going to be down for scheduled maintenance or some other system problem, an email will be sent to the PLEA's *Technical Liaison or Designee* by the MDPD administrator of the PI System.

IX. TRAINING:

Initial training and online user manuals will be provided to the PLEA's *Technical Liaison or Designee*. The *Technical Liaison or Designee* will then be responsible for fully training all of the PLEA's users. The MDPD holds annual PI System training at the MDPD Fred Taylor Headquarters building. An email notification will be sent approximately a month prior to the training along with information on the times and location. Applicants will be selected on a first come, first serve basis and all users are invited to attend. Requests will be taken via e-mail sent to PI.SUPPORT@mdpd.com, and approved by MDPD. If additional training is required, please contact the System Administrator for assistance at PI.SUPPORT@mdpd.com.

It is very important that training be made available to users, specifically on the "facial recognition" component of the PI System. Although the facial recognition process is relatively simple, there are key points that must be understood for the user to have the greatest possibility for success when using this component.

X. THE PI SYSTEM:

- A. The PI System shall be used, at all times, by the PLEA in a manner consistent with its intended function as described herein.

This application provides the PLEA access to adult and juvenile arrest images, data for arrestees booked via the MDCRD Pre-Trial Detention Center, MDCRD Turner Guilford Knight Correctional Center, and the JAC. The images and data are stored in the MDPD PI System server database and will allow law enforcement personnel to perform investigative searches, create photo line-ups, search electronic mug-books, create BOLO announcements, perform facial recognition searches, and access composite drawings. The PLEA will be granted software licenses for an unlimited number of users within the Miami-Dade County geographical boundaries for the following two products:

- **Dataworks Plus (DWP): Web Retrieve Software**
This software will allow searches on multiple databases by any of the fields visible on the screen, it will allow creation of lineups, lineups in witness mode, creation of BOLO, perform Facial Recognition on a JPEG image, produce adhoc (listing) reports.
- **Dataworks Plus, Web Palm Software (PDA usage)**
The PDA software will allow retrieval of any record from available databases. The insertion of records/images however via PDA will require a license (with associated costs) and access to a specific user database.

Please note: The application is being provided with current retrieval functionality without any licensing charge to the user agency. If a specific report or additional functionality to the application is requested beyond what is being offered, there might

be a cost associated with the request. The cost will be based per existing contract cost with DWP and Miami-Dade County at a rate of \$140 per hour. The result of the request could be considered a shared item with the rest of all users (law enforcement agencies) within Miami-Dade County.

The use of this system will help the day-to-day operation of the PLEA and will allow the MDPD to facilitate a long-term plan for providing this service to other municipal police agencies within Miami-Dade County. The MDPD will continue to work with the PLEA to ensure the maintenance and expansion of the various systems.

The PLEA will ensure that each authorized user has a unique "User ID" and password to access the application. Under no circumstances shall this "User ID" and password be shared with any other individual.

The notification to destroy any picture/data regarding a printed inmate record from the PI System that has been lawfully expunged will be based on appropriate Court Orders. The user will be sent a notification to destroy the image/data via email as required by Florida State Statutes 943.0585.

B. The Rapid Identification System shall be used, at all times by the PLEA in a manner consistent with its intended function as described herein.

MDPD will make available access to FDLE's criminal history check and the Federal Bureau of Investigation Repository for Individuals of Special Concern (RISC) using the Rapid ID equipment via the current PI System connection. The Dataworks Plus Rapid ID equipment (as approved by FDLE) connects to the PI System via the Rapid ID server. This device performs a two finger print check for criminal history of the individual, including state and out-of-state warrants. The connections via the PI System for the Rapid ID is unlimited for the PLEA, including the reporting capability of the PI System. There is no charge for the connection between the PLEA and our FDLE Rapid ID server.

Rapid ID device(s) will need to be purchased by the PLEA from Dataworks Plus under the Florida State contract. The purchase of the unit(s) and maintenance agreement will be made between the participating agency and Dataworks Plus.

The MDPD has made connection with users of Dataworks Plus systems via the High Intensity Drug Trafficking Area (HIDTA) in New York City which currently includes Pennsylvania, New Jersey, New York, and Michigan. There are future plans to add other databases from different areas of the United States. These additional databases will also be made available through the PI System to PLEA within Miami-Dade County and will be covered by this amendment.

The connection to HIDTA will follow the protocol below:

- 1) A user who prints a record (image/data) that later becomes sealed or expunged will receive an email advising the user of a print that has become sealed or expunged. He is further instructed to comply as per the MOU to destroy the printed document that is now sealed or expunge.
- 2) A monthly word document will be provided to the PLEA's Technical Liaison advising the liaison of the users that have printed a sealed or expunged record. The liaison will save the document to his computer and then insert his/her name in the signature box in the bottom of the page which will attest to the fact the requested action has been completed by the users on the list. The signed document will then be emailed back to the MDPD system administrator at

PI.SUPPORT@MDPD.com, who will then forward the signed document to HIDTA.

- 3) The next time the user logs in to the PI System the user will be prompted with the question of whether the user has destroyed the printed document. If the response is "No", the user will not be allowed to log in. If the user's response to the question is "Yes", the user will be allowed to proceed with the log in.

Rapid ID PLEAs will follow the guidelines set forth by FDLE by:

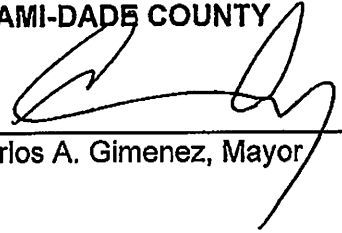
- 1) Providing training on the use of the equipment.
- 2) Creating a Standard Operating Procedure (SOP) of when the equipment is to be used and providing each participating officer with a copy of the SOP.
- 3) Following the Florida Statutes regarding traffic or investigative stops.
- 4) Possessing FDLE Florida Crime Information Center (FCIC)/National Crime Information Center (NCIC) certification.
- 5) Following FDLE Florida Crime Information Center (FCIC)/National Crime Information Center (NCIC) certification.

XI. EFFECTIVE DATE AND TERMINATION:

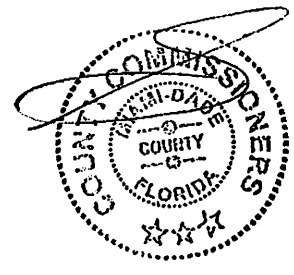
This MOU becomes effective upon signature of both parties and will remain in full force and effect until rescinded by either party in writing. This MOU may be terminated by either party, with or without cause, by giving 30 day advanced written notice to the other party. Said notice shall be sufficient if it is delivered to the party personally, mailed by certified mail, or sent by facsimile.

IN WITNESS THEREOF, the subscribing officials are authorized to acknowledge and execute this MOU on behalf of their agency.


MIAMI-DADE COUNTY



Carlos A. Gimenez, Mayor *for* Date 7/16/13



MIAMI-DADE POLICE DEPARTMENT



for J.D. Patterson, Director Date 7/5/2013

PARTICIPATING LAW ENFORCEMENT AGENCY (PLEA)

Doral Police Department

Agency Name

Donald W. DeLucca, Chief

Agency Representative Name



Agency Representative Signature

Date

**Approved as to form and legal sufficiency
for the sole use of the City of Doral.**



City Attorney



Print Name

TECHNICAL LIAISON – PARTICIPATING LAW ENFORCEMENT AGENCY (PLEA)

Agency: Doral Police Dept.

Name: Cathy Jewett

Title: Sergeant

Office Phone Number: (305) 593-6099, ext. 2111

Cell Phone Number: (786) 255-1309

Email Address: Cathy.Jewett@doralpol.com

FBI Form

APPENDIX H SECURITY ADDENDUM

Instructions:

Federal Bureau of Investigation (FBI) Criminal Justice Information Services Security Addendum

Please complete the FBI form as follows:

1. Have the appropriate person(s) sign and date for the respective law enforcement agency partner. The FBI has provided space for two signatures, labeled:
 - *The "Contractor" is the Police Law Enforcement Agency (PLEA).*
 - *"Printed Name/Signature of Contractor Employee"*
This would be the personnel assigned as your agency Security Officer for law enforcement information systems.
 - *"Printed Name/Signature of Contractor Representative"*
This is the agency head, i.e. Chief of Police.
2. Enter the "Organization and Title of Contractor Representative" on the appropriate line.
3. Return the original signature FBI Criminal Justice Information Services Security Addendum to the Miami-Dade Police Department with the Memorandum of Understanding (three original signatures) to:

Ms. Susan Windmiller
Miami-Dade Police Department
9105 N.W. 25th Street, Suite 3042
Miami, Florida 33172-1500

For questions, contact Ms. Windmiller, of the Miami-Dade Police Department's Police Legal Bureau as 305-471-3197.

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

- 4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.
- 4.02 Security violations can justify termination of the appended agreement.
- 4.03 Upon notification, the FBI reserves the right to:
- a. Investigate or decline to investigate any report of unauthorized use;
 - b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Cathy Jewett

Printed Name/Signature of Contractor Employee

6-9-15

Date

[Signature]

Printed Name/Signature of Contractor Representative

6-9-15

Date

Doral Police Dept.; Chief of Police

Organization and Title of Contractor Representative

RESOLUTION No. 15-98

A RESOLUTION OF THE MAYOR AND THE CITY COUNCIL OF THE CITY OF DORAL, FLORIDA APPROVING A MEMORANDUM OF UNDERSTANDING BETWEEN MIAMI-DADE COUNTY AND THE CITY OF DORAL FOR PHOTO IMAGING SYSTEM ACCESS VIA THE WEB THROUGH SECURED AGENCY INTRANET ACCESS; PROVIDING FOR IMPLEMENTATION; AND PROVIDING FOR AN EFFECTIVE DATE

WHEREAS, Miami-Dade County (the "County") owns and operates computerized Photo Imaging System (the "Imaging System") for law enforcement use, which the City of Doral (the "City") desires to use; and

WHEREAS, the Imaging System and related components consist of booking photographs along with data related to personal property, arrest date of arrested individuals (adults/juveniles) that have been processed by the Miami-Dade Corrections and Rehabilitation Department, and the Juvenile Assessment Center, which is processed and updated in real-time; and

WHEREAS, the Imaging System is a web based system that allows other law enforcement agencies in Miami-Dade County to have access via the web through a secured agency intranet access; and

WHEREAS, the County has established a Memorandum of Understanding, which is attached hereto as Exhibit "A" and incorporated herein and made a part hereof by this reference (the "MOU"), by which it grants other enforcement agencies the permission to utilize the Imaging System, in accordance with certain protocols, procedures, and obligations; and

WHEREAS, Staff has recommended that the City Council approve MOU between Miami Dade County and the City of Doral to utilize the Radio System for police operations.

NOW THEREFORE, BE IT RESOLVED BY THE MAYOR AND CITY COUNCIL OF THE CITY OF DORAL AS FOLLOWS:

Section 1. Recitals. The above recitals are confirmed, adopted, and incorporated herein and made a part hereof by this reference.

Section 2. Approval. The Memorandum of Understanding between Miami Dade County and the City of Doral for the use of the Imaging System, which is attached hereto as Exhibit "A", is hereby approved. The City Manager is hereby authorized to execute the MOU on behalf of the City, subject to approval as to form and legal sufficiency by the City Attorney.

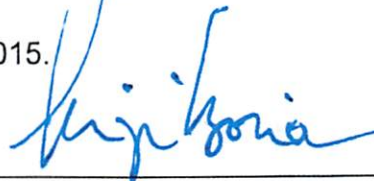
Section 3. Implementation. The City Manager and the City Attorney are hereby authorized to take such further action as may be necessary to implement the purpose and provisions of this Resolution.

Section 4. Effective Date. This Resolution shall become effective immediately upon its adoption.

The foregoing Resolution was offered by Vice Mayor Ruiz who moved its adoption. The motion was seconded by Councilmember Rodriguez and upon being put to a vote, the vote was as follows:

Mayor Luigi Boria	Yes
Vice Mayor Sandra Ruiz	Yes
Councilman Pete Cabrera	Yes
Councilwoman Christi Fraga	Yes
Councilwoman Ana Maria Rodriguez	Yes

PASSED AND ADOPTED this 13 day of May, 2015.



LUIGI BORIA, MAYOR

ATTEST:



CONNIE DIAZ, CITY CLERK

APPROVED AS TO FORM AND
LEGAL SUFFICIENCY FOR THE SOLE USE
OF THE CITY OF DORAL



WEISS, SEROTA, HELFMAN, COLE, & BIERMAN, PL
CITY ATTORNEY