INTERLOCAL COOPERATION AGREEMENT

THIS INTERLOCAL COOPERATION AGREEMENT is made and entered into effective this ___2___day of _____JUNE_____, 2015, by and between the county of Moore (the "County" herein) and county of Hidalgo, Hidalgo County Sheriff's Office (the "Entity" herein), political subdivisions of the State of Texas.

WITNESSETH:

WHEREAS, V.T.C.A., Government Code, Chapter 791, the Texas Interlocal Cooperation Act, provides that any one or more local governmental entities may contract with each other for the performance of governmental functions and for the joint use of facilities or services for police protection and for the promotion and protection of the health and welfare of the inhabitants of this State and the mutual benefit of the parties;

WHEREAS, the County, for purposes of performing functions of law enforcement through its Sheriff's Office, has an authorized access terminal providing access to the Texas Law Enforcement Telecommunications System ("TLETS");

WHEREAS, TLETS provides potentially valuable law enforcement-related data from intrastate and interstate sources to assist law enforcement in the investigation of crime;

WHEREAS, TLETS is administered by the Texas Department of Public Safety, who in turn grants specific access to TLETS through specifically defined terminals, one of which is held by the County through its Sheriff's Office;

WHEREAS, the Entity desires to access TLETS through the current authorized connection of the County to assist the Entity in the investigation of crime;

WHEREAS, the Entity's investigation of crime serves the purpose of providing police protection and promoting and protecting the health and welfare of local residents;

WHEREAS, the County, by its proximity, will benefit from improved criminal investigation by the nearby Entity; and

WHEREAS, the County desires to allow the Entity to access TLETS through the County's authorized connection for criminal justice purposes by the Entity, with the Entity bearing any additional costs related to the Entity gaining access to TLETS through the County.

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the undersigned parties agree as follows:

I. Terms and Conditions

1. County agrees to allow Entity to access County's authorized TLETS connection for criminal justice purposes.

2. Entity agrees to bear any costs associated with Entity gaining access to and using County's TLETS connection.

3. Entity agrees that Entity's use of County's TLETS connection and information obtained therefrom shall at all times comply with all applicable local, state, and federal regulations.

4. Entity agrees that if County determines, in its sole and absolute discretion, that Entity's connection with County's TLETS connection has any negative affect on County's computer network, terminals, operations, or any administrative function of the County or the County's Sheriff's Office, then County may terminate this Agreement and remove Entity's connection to TLETS. In the event of such termination of this Agreement and the server connection, County shall bear no cost or liability to Entity and the indemnification of Section 2 of Article II shall remain in full force and effect.

II. Miscellaneous

1. The parties agree that in the event any provision of this Agreement is held by a court of competent jurisdiction to be in contradiction of any laws of the State or the United States, the parties will immediately rectify the offending portions of this Agreement. The remainder of the Agreement shall be in full force and effect.

2. The Entity will indemnify and hold harmless the County, its officers, agents, servants and employees from and against any and all suits, actions, legal proceedings, claims, demands, damages, costs, expenses, and attorney's fees, arising out of a willful or negligent act or omission of the Entity, its officers, agents, servants and employees under this Agreement; provided, however, that this indemnity shall not apply to any claims, demands, damages, costs, expenses and attorneys' fees arising out of this Agreement based upon any willful or negligent act or omission of the County, its officer, agents, servants and employees.

3. Any financial obligations of the parties under this agreement shall be payable from current revenues available to the respective paying party.

4. This Agreement constitutes the entire agreement between the parties hereto, and supersedes all of their oral and written negotiations, agreements and understandings of every kind. The parties understand, agree and declare that no promise, warranty, statement or representation of any kind whatsoever, which is not expressly stated in this Agreement, has been made by any party hereto or its officers, employees or other agents to induce execution of this Agreement. This Agreement cannot be modified, or any of the terms hereof waived, except by an instrument in writing, referring specifically to this Agreement, executed by the parties.

5. The laws of the State of Texas shall govern the validity, enforcement and interpretation of this Agreement. The obligations of the parties are performable and venue for any legal action arising out of this Agreement shall lie in Moore County, Texas.

6. This Agreement shall be binding upon and inure to the benefit of the County and the Entity and their respective representatives, successors and assigns. Except as expressly provided herein, nothing in this Agreement is intended to confer on any person, other than the parties hereto and their respective heirs, personal representatives, successors and assigns, any rights or remedies under or by reason of this Agreement.

7. In addition to the acts recited in this Agreement to be performed by any party, the parties agree to perform, or cause to be performed, any and all such further acts as may be reasonably necessary to consummate the acts or transactions contemplated hereby.

8. The effective date of this Agreement shall be the date of the last of the parties to approve and ratify this Agreement.

County of Moore, Texas

Approved and entered into on the ____ day of _____, 2015.

_____

ATTEST:

_____

County of Hidalgo, Hidalgo County Sheriff's Office, Texas

Approved and entered into on the __2__ day of _____JUNE_____, 2015.

_____

ATTEST:

_____

Texas Signatory Page

The undersigned parties agree that the *Security Addendum* is now a part of the contract between the entities. The parties agree to abide by all requirements of the *Security Addendum* and the *CJIS Security Policy*, and it shall remain in force for the term of the contract. Any violation of this addendum constitutes a breach of the contract.

To the extent there is a conflict between a confidentiality clause in the underlying contract and the *Security Addendum* and/or the *CJIS Security Policy*, the *Security Addendum* and the *CJIS Security Policy* shall govern any information covered by the *Security Addendum* and/or the *CJIS Security Policy.*

(To be signed and dated by the vendor and law enforcement agency representative(s) who signed the original contract, or at least who have authority to bind each entity.)

RICHARD OZUNA
Printed Name of Agency Representative

	CAPTAIN
Signature of Agency Representative	Title
HIDALGO COUNTY SHERIFF TX1080000	
Agency Name and ORI	Date

John H. Greene Jr.
Printed Name of Vendor (Contractor) Representative

	Vice President of Operations
Signature of Vendor (Contractor) Representative	Title
COPsync, Inc.	
Vendor Organization Name	Date

Non-Satellite Based Computing Device Agreement

This document is a request by Hidalgo County Sheriff's Office (Hosted Agency) of the CJIS System Agency (CSA) for the State of Texas, the Texas Department of Public Safety, for the purpose of hosting State and Federal Criminal Justice data over 30 (# MDTs) 8 (# desktops) internet based device(s) that connect to the State network through equipment at Moore County Sheriff's Office (Hosting Agency). The Hosted Agency is responsible for meeting all the requirements of the CJIS Security Policy and NCIC Operating Manual at all times regarding training, network security, physical security, and any other requirements specified in the policies and by the CSA for these devices. The Hosted Agency understands that they will be audited by the CSA regarding their usage of these internet based devices at any time at the discretion of the CSA.

The Hosted Agency understands that they are responsible for ensuring that all system users are identified by a unique user ID and compliant password. All computers connected to the CSA's systems shall be protected by a firewall and ensure that the operating system is kept current regarding security updates. Antivirus software must be used at all times and be updated frequently. If the computing device may be used outside of a secure location, the Hosted Agency must ensure that advanced authentication as defined by the CJIS Security Policy is employed. The CJIS Security Policy currently defines a secure location as a criminal justice facility or a police vehicle.

The Hosted Agency understands that failure to comply with any current or future requirements of the CJIS Security Policy, the NCIC Operating Manual, or any policies required by the CSA will be cause for immediate termination of service at the Hosting Agency. Service will remain terminated until such time as the Hosted Agency can demonstrate their ability to remain fully compliant. This determination shall be at the sole discretion of the CSA.

Hosted Criminal Justice Agency	**Approved for _____ devices:**
_____	_____
Signature	Signature
RICHARD OZUNA	
Printed Name	Printed Name
CAPTAIN	
Title	Title
6/02/2015	
Date	Date

Agency Identification

Agency Name	ORI
HIDALGO COUNTY SHERIFF OFFICE	TX1080000
Agency Address	
711 EL CIBOLO ROAD	
City	**Zip**
EDINBURG	78539
Agency Representative (Title and Name)	
CAPTAIN RICHARD OZUNA	
Phone Number	**Fax Number**
956-393-6031	
Email address	
richard.ozuna@hidalgoso.org	

Contractor Identification

Company Name		
COPSYNC, INC		
Company Address		
1000 N. WALNUT SUITE 150		
City	**State**	**Zip**
NEW BRAUNFELS	TX	78130
Contractor Representative (Title and Name)		
ANN ARNOLD/ CUSTOMER PROCUREMENT AND INSTALLATION SPECIALIST		
Phone Number	**Fax Number**	
(972) 865-6192 EXT: 7466	(972) 201-9647	
Email address		
aarnold@copsync.com		

Submit hard copies and any applicant finger print cards to:

Via USPS:
Texas Department of Public Safety
CJIS Security Office \ Information Technology
P O Box 4143 MSC 214
Austin, TX 78765-4143

Via overnight carrier:
Texas Department of Public Safety
CJIS Security Office \ Information Technology
5805 N. Lamar, Bldg. G
Austin, TX 78752

Email can be sent to: Security.Committee@txdps.state.tx.us

Main office number is: (512) 424-5686

Parties may use the following Security Addendum with the Texas Signatory Page or, in their contract, choose to incorporate the Security Addendum by reference. If the Addendum is incorporated by reference into the contract, a copy of the contract must be provided to the TX DPS CJIS Security Office.

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.

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), 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 2000 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.

_____ _____
Signature of Contractor Employee Date

_____
Printed or Typed Contractor Employee Name

Sex: ____ Race: _____ DOB: _____ State/ID or DL: _____

_____ _____
Signature of Contractor Representative Date

John H. Greene Jr.
Printed or Typed Name of Contractor Representative

COPsync, Inc. / Vice President of Operations
Organization Name and Representative's Title