Exhibit 1

FIRST AMENDMENT TO AGREEMENT BETWEEN BROWARD COUNTY AND SUNGARD PUBLIC SECTOR, INC.

This First Amendment ("First Amendment") to the Agreement Between Broward County and SunGard Public Sector, Inc. is entered into by and between Broward County, a political subdivision of the State of Florida ("County"), and CentralSquare Technologies, LLC, f/k/a Sungard Public Sector, Inc., a Delaware corporation authorized to transact business in the State of Florida ("CentralSquare") (collectively County and CentralSquare are referenced as the "Parties").

RECITALS

A. On or about August 31, 2009, the Broward County Sheriff's Office ("BSO") entered into an agreement with SunGard Public Sector, Inc. ("SunGard") for licensing of certain application software from SunGard to operate and maintain a regional records management system (as amended, the "BSO Agreement").

B. On or about June 20, 2013, BSO, County, and SunGard executed a Partial Assignment, Delegation, and Release Agreement (the "Assignment") which assigned portions of the BSO Agreement to County. The applicable portions of the BSO Agreement assigned by BSO to County, as updated and amended by the Assignment, are referred to as the "Agreement" herein.

C. Annual support services for the licensed software provided to County under the Agreement expires September 30, 2020.

D. On or about September 15, 2018, SunGard Public Sector, Inc., merged with other entities into CentralSquare Technologies, LLC. As part of the merger, CentralSquare assumed all rights, obligations, and liabilities of SunGard as it relates to the Agreement.

E. The Parties desire to amend the Agreement to extend the term for annual support services, increase the applicable not-to-exceed amounts, update and clarify the software covered under the Agreement, and amend certain other provisions.

Now, therefore, for good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, County and CentralSquare agree as follows:

1. The above Recitals are true and correct and are incorporated herein by reference. All capitalized terms not expressly defined within this First Amendment shall retain the meaning ascribed to such terms in the Agreement. All references in the Agreement to SunGard shall be deemed to refer to CentralSquare, and all references to County's Office of Communications Technology shall be deemed to refer to County's Regional Emergency Services and Communications division.

2. Except as modified herein, all terms and conditions of the Agreement remain in full force and effect.

3. The Parties wish to clarify the current status of the Exhibits of the Agreement based on certain changes that were agreed to, via the Assignment, as it relates to the BSO Agreement. Specifically, the Assignment:

a) Replaced Exhibit A ("Agency Access Agreement") of the BSO Agreement in its entirety. All references to Exhibit A of the Agreement shall be deemed to refer to Exhibit A of the Assignment.

b) Updated the list of Licensed Software listed in Exhibit B of the BSO Agreement and identified:

i. The "Assigned Licenses" in Schedule B1 and the additional software modules licensed to County in Schedules B2 and B3 (collectively, the "County Licensed Software"); and

ii. The software modules retained by BSO in Schedules C1, C2, C3, and C4.

All references to Exhibit B of the Agreement shall be deemed to refer to Schedules B1, B2, and B3, collectively.

c) Attached in Exhibit D the minimum workspace specifications referenced in Exhibit C of the BSO Agreement. Any references to Exhibit C of the BSO Agreement shall be deemed to refer to Exhibit C of the BSO Agreement as supplemented by Exhibit D of the Assignment.

d) The Assignment added Exhibit I to the BSO Agreement. Any reference to Exhibit I of the Agreement shall be deemed to refer to Exhibit I of the Assignment. Exhibits D, E, F, and H of the BSO Agreement remained unchanged. Any reference to Exhibits D, E, F, and H of the Agreement shall be deemed to refer to Exhibits D, E, F, and H of the BSO Agreement.

e) Attached Exhibit E as an addition to Exhibit G of the BSO Agreement. Any references to Exhibit G of the Agreement shall be deemed to refer to Exhibit G of the BSO Agreement as supplemented by Exhibit E of the Assignment.

4. The Parties wish to amend the Agreement to replace Exhibit B (i.e., Schedules B1, B2, and B3) in its entirety with the attached Exhibit B, which updates the list of "County Licensed Software" and sets forth the associated annual support services fees.

5. The Parties wish to amend the Agreement to replace Exhibit E in its entirety with the attached Exhibit E, which updates the support services provisions applicable to the County Licensed Software.

6. Section 10.1 of the Agreement provided for annual support services through September 30, 2020. The Parties wish to extend annual support services for five (5) additional years from October 1, 2020, through September 30, 2025 (the "2020-2025 Term"). Upon execution of this First Amendment, the Parties agree that support services, as set forth in Exhibit E, shall continue for the 2020-2025 Term, unless terminated pursuant to Section 16.1 of the Agreement

7. County will pay CentralSquare up to a maximum not-to-exceed amount of $350,000.00 for support services for the duration of 2020-2025 Term (annual support services fees set forth in Exhibit B). County will pay CentralSquare up to a maximum not-to-exceed amount of $70,000.00 for "Optional Services" for the duration of the 2020-2025 Term. Optional Services refers to any software licenses and modules that County may elect to acquire through a Work Authorization related to the software set forth in Exhibit B, as well as any professional services related to implementation of same (see Exhibit G), and includes training, consulting, and other technical matters related to the licensed software.

8. The Agreement is amended to replace Exhibit G in its entirety with the attached Exhibit G ("Optional Services Pricing").

9. The Agreement is amended to add Exhibit J, "Minimum Security Requirements." CentralSquare and all software and services provided under the Agreement shall comply at all times with Exhibit J.

10. County entered into a Criminal Justice Information Security Addendum, dated July 1, 2019, with a subsidiary of CentralSquare. The Agreement is amended to add Exhibit K, "CJIS Addendum." As of the effective date of this First Amendment, CentralSquare shall comply with all terms set forth in Exhibit K, which shall supersede the addendum dated July 1, 2019.

11. The effective date of this First Amendment shall be the date of complete execution by both Parties.

12. This First Amendment may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

(The remainder of this page is blank.)

IN WITNESS WHEREOF, the Parties hereto have made and executed this Agreement: BROWARD COUNTY through its BOARD OF COUNTY COMMISSIONERS, signing by and through its Mayor or Vice-Mayor, authorized to execute same by Board action on the _____ day of _____, 2020, and CENTRALSQUARE TECHNOLOGIES, LLC, signing by and through its _____, duly authorized to execute same.

BROWARD COUNTY

ATTEST:

_____
Broward County Administrator, as
ex officio Clerk of the Broward County
Board of County Commissioners

BROWARD COUNTY, by and through
its Board of County Commissioners

By_____
Mayor

____ day of _____, 2020

Approved as to form by
Andrew J. Meyers
Broward County Attorney
Governmental Center, Suite 423
115 South Andrews Avenue
Fort Lauderdale, Florida 33301
Telephone: (954) 357-7600
Telecopier: (954) 357-7641

By Neil Sharma Digitally signed by Neil Sharma Date: 2020.08.31 09:30:11 -04'00'
Neil Sharma (Date)
Assistant County Attorney

By Digitally signed by RENE D. HARROD Date: 2020.08.31 10:23:36 -04'00'
René D. Harrod (Date)
Deputy County Attorney

NS/RDH
CentralSquare First Amendment
08/04/2020

FIRST AMENDMENT TO AGREEMENT BETWEEN BROWARD COUNTY AND SUNGARD PUBLIC SECTOR, INC.

CentralSquare

WITNESSES:

DocuSigned by:
Danilo Gargiulo
Signature

Danilo Gargiulo
Print Name of Witness

DocuSigned by:
Christopher Copeland
Signature

Christopher Copeland
Print Name of Witness

CENTRALSQUARE TECHNOLOGIES, LLC

By DocuSigned by:
David Gai
Authorized Signor

David Gai Chief Customer Officer
Print Name and Title

_____ day of 8/27/2020, 2020

ATTEST:

DocuSigned by:
Barry Medintz
Corporate Secretary or authorized agent

(CORPORATE SEAL)

Exhibit B – Licensed Software and Annual Support Services Fees

Licensed Software (each quantity: 1 enterprise license)	Support Services Annual Fee (Invoiced Quarterly in Arrears) 10/1/2020 – 9/30/2021*	Quarterly Invoice amount 10/1/2020 – 9/30/2021
OSSI Police to Police Annual Subscription Fee	Included at no cost	Included at no cost
OSSI Client Base Records Management System	Included at no cost	Included at no cost
OSSI Base Mobile Server Software Client	Included at no cost	Included at no cost
OSSI Multi-Jurisdictional RMS Option	$1,109.14	$277.29
OSSI First RMS Map Display and Map Maintenance Software License	$1,109.14	$277.29
OSSI Basic Accident Module	$1,714.14	$428.54
OSSI Accident Wizard Base Server License	$1,008.28	$252.07
OSSI Felony Registration Module	$1,512.47	$378.12
OSSI Notification Module	$4,537.44	$1,134.36
OSSI Calls for Service Module	$1,512.47	$378.12
OSSI's Integrated Messaging Software Switch	$6,272.84	$1,568.21
OSSI - OPS RMS	$5,041.62	$1,260.41
OSSI RMS Custom Modification-Motorola UDT/RDW to CFS	$2,016.65	$504.16
OSSI RMS Custom Modification - Arrest Interface	$1,512.47	$378.12
OSSI RMS Custom Modification - Warrants Interface	$1,008.28	$252.07
OSSI Bike Registration Module	$447.00	$111.75
OSSI Traffic Citation Module	$546.74	$136.69
OSSI Field Contacts	$447.00	$111.75
OSSI Generic Permit Module	$497.43	$124.36
OSSI Mugshot Capture Station Software Only	$546.74	$136.69
OSSI Parking Ticket Administration Module	$746.19	$186.55
OSSI Residential Security Watch Module	$447.00	$111.75
OSSI Review Module for Field Reporting	$1,493.41	$373.35
OSSI Ordinance Module	$678.97	$169.74
OSSI Property and Evidence Module	$845.84	$211.46
OSSI Training Module	$746.19	$186.55
OSSI - Link Analysis Module	$6,273.96	$1,568.49
OSSI Sex Offender Module	$2,688.87	$672.22
OSSI - Crime Analysis Plus Module	$6,273.96	$1,568.49
OSSI - Intelligence Module	$1,344.43	$336.11
OSSI - RMS TECHNICAL PROFESSIONAL SERVICES (SUPPORT)-Replication Server	$2,694.20	$673.55
OSSI Police to Police Data Host License	Included at no cost	Included at no cost
OSSI RMS Canine Tracking Module	$740.55	$185.14
OSSI - RMS - Daily Activity Module - Enterprise	$2,016.65	$504.16

Licensed Software (each quantity: 1 enterprise license)	Support Services Annual Fee (Invoiced Quarterly in Arrears) 10/1/2020 – 9/30/2021*	Quarterly Invoice amount 10/1/2020 – 9/30/2021
OSSI Document Scanning and Storage	$2,036.83	$509.21
OSSI Agency Asset Management Module	$1,731.27	$432.82
OSSI Crime Analysis Module - Client License	$2,546.00	$636.50
Total	**$64,144.16**	**$16,036.04**

*These amounts will remain the same for the duration of the 2020-2025 Term unless increased pursuant to this paragraph. CentralSquare may increase the annual support service fee for the listed licensed software on an annual basis, starting October 1, 2021, and each year thereafter for the duration of the 2020-2025 Term, with thirty (30) days' advance written notice to County (i.e., no later than September 1 for the upcoming October 1 anniversary), provided that such increase per annum shall not exceed the lesser of 3% or current CPI. The increase or decrease in CPI shall be calculated as follows: the difference of CPI current period less CPI previous period, divided by CPI previous period, times 100. The CPI current period shall mean the most recent published monthly index prior to Agreement anniversary. The CPI previous period shall mean for the same month of the prior year. All CPI indices shall be obtained from the U.S. Department of Labor table for Consumer Price Index – All Urban Consumers (Series ID CUURA320SA0) for the area of Miami-Fort Lauderdale, FL (All Items), with a base period of 1982-1984 = 100, and not seasonally adjusted.

Exhibit E – Support Services

I. **Support Hours: Hours During Which CentralSquare's Telephone Support Will be Available to County in Connection with the Provision of Maintenance:** Unless otherwise noted in the order as to support type, Support Services hours are Monday through Friday, 8:00 A.M. to 5:00 P.M. County's local time within the continental United States, excluding holidays ("5x9").

II. **Targeted Response Times**: "Notification" means a communication to CentralSquare's help desk by means of: (i) CentralSquare's web helpline; or (ii) the placement of a telephone call.

III. **Support Terms:** CentralSquare shall provide the ongoing Support Services described herein for the corresponding Fees outlined in Exhibit B.

With respect to CentralSquare's support obligations, CentralSquare will use diligent, commercially reasonable efforts to respond to Notifications from County relating to the Software identified in Exhibit B in accordance with the following guidelines with the time period to be measured beginning with the first applicable CentralSquare "Telephone Support" hour occurring after CentralSquare's receipt of the Notification:

Priority	Description	Response Goal	Resolution Goal
Urgent 1	A support issue shall be considered **Urgent** when it produces a Total System Failure; meaning the Solution is not performing a process that has caused a complete work stoppage.	Within 60 minutes of the issue being reported and a resolution planned within 24 hours.	Although resolution times vary depending on the exact issue and County environment, CentralSquare has a stated goal to resolve an urgent issue within 24 hours or provide a resolution plan with urgent issues within 24 hours of being reported. A resolution plan will detail the steps necessary to understand and possibly resolve the issue.
Critical 2	A support issue shall be considered **Critical** when a critical failure in operations occurs; meaning CentralSquare 's Solution is not performing a critical process and prevents the continuation of basic operations. Critical problems do not have a workaround. This classification does not apply to intermittent problems.	Within two hours of the issue being reported and a resolution planned within five (5) days.	
Non-Critical 3	A support issue shall be considered **Non-Critical** when a non-critical failure in operations occurs; meaning the Solution is not performing non-critical processes, but the system is still usable for its intended purpose or there is a workaround.	Within four hours of the issue being reported.	
Minor 4	A support issue will be considered **Minor** when the issue causes minor disruptions in the way tasks are performed, but does not affect workflow or operations. This may include cosmetic issues, general questions, and how to use certain features of the system.	Within 24 hours of the issue being reported.	

Response timing is measured from the moment a Case number is created. As used herein a "Case number" is created when a) CentralSquare's support representative has been directly contacted by County either by phone, in person, or through CentralSquare 's online support portal, and b) when CentralSquare's support representative assigns a case number and conveys that case number to the County. County must provide remote access to its facility using a CentralSquare approved remote access (in conjunction with Exhibit J) so that CentralSquare can perform the support obligations and/or services under this Agreement. County will provide appropriate security access and accounts for CentralSquare staff and each session participant.

Exhibit G – Optional Services Pricing

Training: $160 per hour
Installation: $175 per hour
Technical Services/Consulting: $200 per hour
Project Management: $160 per hour

Exhibit J – Minimum Security Requirements

Definitions.

As used in this Exhibit J:

"Contractor" means CentralSquare.

"County Confidential Information" means any County Data that includes employee information, financial information, or personally identifiable information for individuals or entities interacting with County (including, without limitation, social security numbers, birth dates, banking and financial information, and other information deemed exempt or confidential under state or federal law or applicable regulatory body).

"County Data" means the data and information (including text, pictures, sound, graphics, video and other data) relating to County or its employees or agents, or made available or provided by County or its agents to Contractor, for or in the performance of this Agreement, including all derivative data and results derived therefrom, whether or not derived through the use of the Contractor's services, whether or not electronically retained, and regardless of the retention media.

"Equipment" means the hardware being provided by Contractor under the Agreement, if any.

"Software" means software provided or licensed by Contractor pursuant to the Agreement.

All other capitalized terms not expressly defined within this exhibit shall retain the meaning ascribed to such terms in the Agreement (and if not so defined, then the plain language meaning appropriate to the context in which it is used).

Security and Access. If Contractor will have access to any aspect of County's network via an Active Directory account, onsite access, remote access, or otherwise, Contractor must:

(a) comply at all times with all applicable County access and security standards, policies, and procedures related to County's network, as well as any other or additional restrictions or standards for which County provides written notice to Contractor;
(b) provide any and all information that County may reasonably request in order to determine appropriate security and network access restrictions and verify Contractor's compliance with County security standards;
(c) provide privacy and information security training to its employees with access to County's network upon hire and at least once annually; and
(d) notify County of any terminations or separations of Contractor's employees who had access to County's network.

In addition, for any remote access to County's network, Contractor must:

(a) utilize secure, strictly-controlled industry standards for encryption (e.g., Virtual Private Networks) and passphrases and safeguard County Data that resides in or transits through Contractor's internal network from unauthorized access and disclosure;
(b) ensure the remote host device used for access is not connected to any other network, including an unencrypted third party public WiFi network, while connected to County's network, with the exception of networks that are under Contractor's complete control or under the complete control of a person or entity authorized in advance by County in writing;

(c) enforce automatic disconnect of sessions for remote access technologies after a specific period of inactivity with regard to connectivity into County infrastructure;
(d) utilize equipment that contains antivirus protection software, an updated operating system, firmware, and third party-application patches, and that is configured for least privileged access;
(e) utilize, at a minimum, industry standard security measures, as determined in County's sole discretion, to safeguard County Data that resides in or transits through Contractor's internal network from unauthorized access and disclosure; and
(f) activate remote access from Contractor and its approved subcontractors into the County network only to the extent necessary to perform services under this Agreement, deactivating such access immediately after use.

If at any point in time County, in the sole discretion of its Chief Information Officer (CIO), determines that Contractor's access to any aspect of County's network presents an unacceptable security risk, or if Contractor exceeds the scope of access required to perform the required services under the Agreement, County may immediately suspend or terminate Contractor's access and, if the risk is not promptly resolved to the reasonable satisfaction of the County's CIO, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to County network to Contractor).

Data and Privacy. To the extent applicable to the services being provided by Contractor under the Agreement, Contractor shall comply with all applicable data and privacy laws and regulations, including without limitation Florida Statutes Section 501.171, and shall ensure that County Data processed, transmitted, or stored by Contractor or in Contractor's system is not accessed, transmitted or stored outside the United States. Contractor shall not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification information (as defined by Florida Statutes Section 501.171, Section 817.568, or Section 817.5685, as amended) that Contractor may receive or otherwise have access to in connection with this Agreement, unless expressly authorized in advance by County. If applicable and requested by County, Contractor shall ensure that all hard drives or other storage devices and media that contained County Data have been wiped in accordance with the then-current best industry practices, including without limitation DOD 5220.22-M, and that an appropriate data wipe certification is provided to the satisfaction of the Contract Administrator.

Managed or Professional Services. Contractor shall immediately notify County of any terminations or separations of Contractor's employees who performed services under the Agreement and who had access to County Confidential Information or the County network. If any unauthorized party is successful in accessing any information technology component related to Contractor (including but not limited to servers or fail-over servers) where County Data or files exist or are housed, Contractor shall notify County within twenty-four (24) hours after becoming aware of such breach, unless an extension is granted by County's CIO. Contractor shall provide County with a detailed incident report within five (5) days after becoming aware of the breach, including remedial measures instituted and any law enforcement involvement. Contractor shall fully cooperate with County on incident response, forensics, and investigations into Contractor's infrastructure as it relates to any County Data or County applications. Contractor shall not release County Data or copies of County Data without the advance written consent of County. If Contractor will be transmitting County Data, Contractor agrees

that it will only transmit or exchange County Data via a secure method, including HTTPS, SFTP, or another method approved by County's CIO. Contractor shall ensure adequate background checks have been performed on any personnel having access to County Confidential Information. To the extent permitted by such checks, Contractor shall not knowingly allow convicted felons or other persons deemed by Contractor to be a security risk to access County Data. Contractor shall ensure the use of any open source or third-party software or hardware does not undermine the security posture of the Contractor or County.

System and Organization Controls (SOC) Report. Contractor must provide County with a copy of a current unqualified System and Organization Controls (SOC) 2 Type II Report for Contractor that provides the applicable services comprising the system, inclusive of the following Trust Service Principles (Security and Availability), upon audit completion to be completed and provided no later than January 1, 2021, unless this requirement is waived in writing by the County's CIO or designee.

Software Installed in County's Network. To the extent Contractor provides any Software to be installed in County's network, Contractor must:

(a) advise County of all versions of any third-party software (e.g., Java, Adobe Reader/Flash, Silverlight) to be installed and support updates for critical vulnerabilities discovered in applicable third-party or open source software;
(b) ensure that the Software is developed based on industry standards and best practices, including following secure programming techniques and incorporating security throughout the Software-development life cycle;
(c) develop and maintain the Software to operate on County-supported and approved operating systems and firmware versions;
(d) mitigate critical or high risk vulnerabilities (as defined by Common Vulnerability and Exposures (CVE) scoring system) to the Software or Contractor platform within 30 days after patch release, notifying County of proposed mitigation steps to be taken and timeline for resolution if Contractor is unable to apply a patch to remedy the vulnerability;
(e) ensure the Software provides for role-based access controls and runs with least privilege access, enables auditing by default for any privileged access or changes, and supports electronic delivery of digitally signed upgrades from Contractor's or the third-party licensor's website;
(f) ensure the Software is not within three (3) years from its end of life date and provide County with end-of-life-schedules for all applicable Software;
(g) support encryption using at a minimum Advanced Encryption Standard 256-bit encryption keys ("AES-256") or current industry security standards, whichever is higher, for confidential data at rest and use transport layer security (TLS) 1.2 or current industry standards, whichever is higher, for data in motion; and
(h) upon request by County, provide an attestation letter identifying date of the most recent security vulnerability testing performed and any vulnerabilities identified and mitigated (must be dated within six (6) months after any major release).

Equipment Leased or Purchased from Contractor. To the extent Contractor is the Original Equipment Manufacturer (OEM) or an authorized reseller for the OEM for any Equipment provided under this Agreement, Contractor must:

(a) ensure that physical security features to prevent tampering are included in any Equipment provided to County and ensure, at a minimum, industry-standard security measures are followed during the manufacture of the Equipment;
(b) ensure any Equipment provided does not contain any embedded remote-control features unless approved in writing by County's Contract Administrator, and disclose any default accounts or backdoors that exist for access to County's network;
(c) shall supply a patch, firmware update, or workaround approved in writing by County's Contract Administrator within thirty (30) days after identification of a new critical or high security vulnerability and notify County of proposed mitigation steps taken;
(d) develop and maintain Equipment to interface with County-supported and approved operating systems and firmware versions;
(e) upon request by County, make available any required certifications as may be applicable per compliance and regulatory requirements (e.g., Common Criteria, Federal Information Processing Standard 140);
(f) ensure the Equipment is not within three (3) years from its end of life date at the time of delivery and provide County with end-of-life-schedules for all applicable Equipment;
(g) (for OEMs only) support electronic delivery of digitally signed upgrades of any applicable Equipment firmware from Contractor's or the original Equipment manufacturer's website; and
(i) (for OEMs only) upon request by County, provide an attestation letter identifying date of the most recent security vulnerability testing performed and any vulnerabilities identified and mitigated (must be dated within six (6) months after any major release).

Health Information Portability and Accountability Act. If County determines in its reasonable business judgment that Contractor is a covered entity or business associate or otherwise required to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Contractor shall fully protect all protected health information ("PHI") that is subject to the requirements of 45 C.F.R. §§ 160, 162, and 164 and related statutory and regulatory provisions, as required by HIPAA and HITECH.

Business Associate Agreement. If requested by County, Contractor shall execute County's form Business Associate Agreement (located at http://www.broward.org/Purchasing/Pages/StandardTerms_copy(1).aspx). Contractor shall handle and secure such PHI in compliance with HIPAA, HITECH, and its related regulations and, if required by HIPAA, HITECH, or other laws, shall include in its "Notice of Privacy Practices" notice of Contractor's and County's uses of a client's PHI. The requirement to comply with this provision, HIPAA, and HITECH shall survive the expiration or termination of the Agreement.

Exhibit K – CJIS Addendum

This Criminal Justice Information Security Addendum ("Security Addendum") is entered into by and between Broward County, a political subdivision of the State of Florida ("County"), and the CJIS Contractor identified above (County and CJIS Contractor are referred to collectively as the "Parties").

RECITALS

A. County operates the Regional Public Safety Infrastructure, which includes a portion of computer systems and network infrastructure interfacing directly or indirectly with the State of Florida Criminal Justice Network ("CJNet"), National Crime Information Center ("NCIC"), the Florida Crime Information Center ("FCIC"), and the Interstate Identification Index ("III") for the interstate exchange of criminal history and criminal justice information ("CJI").

B. CJIS Contractor is a contractor or subcontractor providing services to the County pursuant to the Applicable Contract identified above. As part of the services provided by the CJIS Contractor under the Applicable Contract, the CJIS Contractor is required to have certain access to CJI (which may include physical or logical access to same). The Criminal Justice Information Services ("CJIS") Division of the Federal Bureau of Investigation ("FBI") administers the CJIS Security Policy, available at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center, which contains information security requirements, guidelines, and agreements regarding the transmission, storage, and use of CJI.

C. The goal of this Security Addendum document is to augment the CJIS Security Policy to ensure adequate security (as defined by the CJIS Security Policy) 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 CJIS Contractor. The intent of this Security Addendum is to require that the CJIS Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the Applicable Contract is executed), as well as with policies and standards established by the CJIS Advisory Policy Board ("APB").

D. 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, 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 applicable government agencies.

Now, therefore, for good and valuable consideration, the receipt and sufficiency of which is acknowledged, the Parties agree as follows:

1. Acknowledgement and Certification. The CJIS Contractor affirms, by execution of this Security Addendum, that each employee of the CJIS Contractor providing services or with access to the CJI under the Applicable Contract 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 in the form attached hereto as **Attachment 1**. The signed acknowledgments shall remain in the possession of County and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

2. Responsibilities of the CJIS Contractor. The CJIS Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the Applicable Contract is executed and all subsequent versions), as well as with policies and standards established by the CJIS APB.

3. Violations. The County must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the County and the CJIS Contractor. Security violations can justify termination of the Applicable Agreement. 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 County and the CJIS Contractor. Upon termination, the CJIS Contractor's records containing CHRI must be deleted or returned to the County.

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

5. Scope and Authority. This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the CJIS Contractor, the County, CJIS system agencies, and the FBI. The following documents are incorporated by reference and made part of this agreement: (a) the Security Addendum; (b) the NCIC Operating Manual; (c) the CJIS Security Policy; and (d) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6. Additional Terms. The terms set forth in this Security Addendum do not constitute the sole understanding by and between the Parties, but rather augment the provisions of the Applicable Agreement and the CJIS Security Policy to provide a minimum basis for the security of the system and contained information. The Parties acknowledge there may be terms and conditions of the Applicable Agreement that impose more stringent requirements upon the CJIS Contractor.

7. Security Addendum Modifications. The form of this CJIS Security Policy Security Addendum may only be modified with the approval of the FBI. All notices and correspondence to the FBI shall be forwarded by First Class mail to: Information Security Officer, Criminal Justice Information Services Division, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306.

IN WITNESS WHEREOF, the parties hereto have made and executed this Assignment Agreement: BROWARD COUNTY through its BOARD OF COUNTY COMMISSIONERS, signing by and through its County Administrator, duly authorized to execute same by Board action on January 29, 2019, Agenda No. 32, and the CJIS Contractor, signing by and through its _____, duly authorized to execute same.

COUNTY

WITNESS:

_____
(Signature)

_____
(Print Name of Witness)

_____
(Signature)

_____
(Print Name of Witness)

BROWARD COUNTY, by and through its County Administrator

By_____
County Administrator

____ day of _____, 2020

Approved as to form by
Andrew J. Meyers
Broward County Attorney
Governmental Center, Suite 423
115 South Andrews Avenue
Fort Lauderdale, Florida 33301
Telephone: (954) 357-7600
Telecopier: (954) 357-7641

By_____
René D. Harrod (Date)
Deputy County Attorney

CRIMINAL JUSTICE INFORMATION SECURITY ADDENDUM

CJIS CONTRACTOR

WITNESSES:

DocuSigned by:
Danilo Gargiulo
Signature

Danilo Gargiulo
Print Name of Witness above

DocuSigned by:
Christopher Copeland
Signature

Christopher Copeland
Print Name of Witness above

By: DocuSigned by:
David Gai
Authorized Signor

David Gai Chief Customer Officer
Print Name and Title

_____ day of 8/27/2020, 20___

ATTEST:

DocuSigned by:
Barry Medintz
Corporate Secretary or other person authorized to attest

(CORPORATE SEAL OR NOTARY)

ATTACHMENT 1: 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.

_____ _____

Printed Name/Signature of CJIS Contractor Employee Date

_____ _____

Printed Name/Signature of CJIS Contractor Representative Date

_____

Title of CJIS Contractor Representative