Exhibit 2

FIRST AMENDMENT TO SYSTEM AND SERVICES AGREEMENT BETWEEN BROWARD COUNTY AND MISSION CRITICAL SYSTEMS, INC.

This First Amendment ("First Amendment") to the System and Services Agreement Between Broward County and Mission Critical Systems, Inc. ("Agreement"), is entered into by and between Broward County, a political subdivision of the State of Florida ("County"), and Mission Critical Systems, Inc., a Florida corporation ("Provider") (collectively County and Provider are referenced as the "Parties").

RECITALS

A. The Parties entered into the Agreement, dated June 6, 2017, for Check Point firewall equipment, software, and support utilized by County in connection with firewall and security administration of County's computer networks.

B. The Parties wish to amend the Agreement to increase the applicable not-to-exceed amounts to account for County's need for additional Check Point firewall equipment, software, and related professional services and Support and Maintenance Services to protect County's computer networks.

Now, therefore, for good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, County and Provider 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.

2. Except as modified herein, all terms and conditions of the Agreement remain in full force and effect. Amendments are indicated herein by use of strikethroughs to indicate deletions and bold/underlining to indicate additions, unless otherwise indicated herein.

3. Section 5.1 of the Agreement is amended as follows:

5.1 For the duration of the Agreement, County will pay Provider up to the following maximum amounts:

Services/Goods	Term	Total Not-To-Exceed Amount
Equipment **(including purchased via purchase order per Section 3.4)**, ~~Subscriptions~~ **Software**, System, and Support and Maintenance Services Per Exhibit A	Initial Term **Each 1 year renewal term (total for two (2) renewal terms)**	~~$1,200,000.00~~ **$2,475,000.00** **$900,000.00 ($1,800,000.00)**
~~Optional renewal terms~~	~~Each 1 year renewal term~~	~~$400,000.00~~

Services/Goods	Term	Total Not-To-Exceed Amount
	~~Total for all renewal terms~~	~~$800,000.00 (2 years)~~
Optional Services **requiring a Work Authorization pursuant to Section 3.4** ~~(including all installations and any Software other than Subscriptions)~~	Duration of the Agreement (inclusive of any renewals)	~~$300,000.00~~ **$500,000.00**
TOTAL NOT TO EXCEED		~~$2,300,000.00~~ **$4,775,000.00**

****

4. Section 9.5 of the Agreement is amended as follows:

9.5 Security and Access. Any access by Provider to any aspect of the County's network must comply at all times with all applicable County access and security standards, as well as any other or additional restrictions or standards for which County provides written notice to Provider. Provider will provide any and all information that County may reasonably request in order to determine appropriate security and network access restrictions and verify Provider's compliance with County security standards. If at any point in time County, in the sole discretion of its Chief Information Officer, determines that Provider's access to any aspect of the County's network presents an unacceptable security risk, County may immediately suspend or terminate Provider's access and, if the risk is not promptly resolved to the reasonable satisfaction of the County's Chief Information Officer, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to the County network to Provider).

~~Provider shall comply with the following either directly or through the performance of Check Point Software Technologies Ltd.:~~

~~a) Upon request by County or as further required in the applicable Work Authorization, Provider shall notify the County of any terminations/separations of employees performing services under the Agreement or who had access to the County's network in order to disable such employees' access to County systems.~~

~~b) Upon request by County or as further required in the applicable Work Authorization, Provider shall ensure all Provider employees have signed County's Information Security Policy Acknowledgement form prior to accessing County network environment. (PCI 12.3.5).~~

~~c) Provider shall perform privacy and information security training upon hire and at least annually to those employees who have access to the sensitive County environment. (PCI 12.6.1)~~

~~d) Provider must provide a security plan or secure configuration guide (i.e., product documentation and specifications) for Software installed in the County environment by the Provider.~~

~~e) To the extent required in the applicable Work Authorization, Provider shall advise of any third party software (e.g., Java, Adobe Reader/Flash, Silverlight) required to be installed and version supported, and support updates for critical vulnerabilities discovered in the versions of that third party software.~~

~~f) Provider shall ensure that the Software is developed based on industry standards/and or best practices, including following secure programming techniques and incorporating security throughout the software-development life cycle.~~

~~g) Provider shall issue an available temporary security patch for newly identified vulnerabilities within 30 days for all critical or high security vulnerabilities and reasonably longer as needed to issue a permanent fix, to ensure it is ready and working.~~

~~h) Provider shall ensure the Software provides for role-based access controls. (i.e., product administration guide for information on role based administration features for that product).~~

~~i) Provider shall support electronic delivery of digitally signed upgrades from Provider or supplier website.~~

~~j) Provider shall enable auditing by default in software for any privileged access or changes.~~

~~k) If the Software is a payment application which processes, stores, or transmits credit card data, the VISA Cardholder Information Security Program ("CISP") payment Application Best Practices and Audit Procedures will be followed and current validation maintained.~~

~~l. Provider shall regularly provide County with access to the end-of-life-schedules for all applicable Software (i.e., Life Cycle Policy announcements, on Check Point's website at https://www.checkpoint.com/support-services/support-life cyclepolicy/#latestannouncements).~~

~~m. Provider shall ensure that physical security features are included in the Hardware acquired under this Agreement to prevent tampering.~~

~~n. Provider shall ensure security measures are followed during the manufacture of the Hardware acquired under this Agreement.~~

~~o. Any Hardware provided under this Agreement shall not contain any embedded remote control features unless approved in writing by County's Contract Administrator.~~
~~p. To the extent default accounts or backdoors exist (if any), Provider shall disclose any default accounts or backdoors for access to County's network.~~

~~q. If a new critical or high security vulnerability is identified, Provider shall issue an available temporary security patch, firmware update or workaround for download via the user center by County's Contract Administrator within 30 calendar days from identification of vulnerability and reasonably longer as needed to issue a permanent fix, to ensure it is ready and working.~~

~~r. Provider shall make available, upon County's request, any required certifications as may be applicable and required (e.g., Common Criteria ("CC"), Federal Information Processing Standard 140 ("FIPS 140").~~

~~s. Provider shall regularly provide County with end-of-life-schedules for all applicable Hardware and Software (i.e., Life Cycle Policy announcements, on Check Point's website at https://www.checkpoint.com/support-services/support-life-cyclepolicy/#latestannouncements).~~

~~t. Provider shall support electronic delivery of digitally signed upgrades from Provider or supplier website (via Check Point user center and support center).~~

~~u. Upon County's request, Provider shall make available to the County proof of Provider's compliance with all applicable federal, state, and local laws, codes, ordinances, rules, and regulations in performing under this Agreement (e.g., ISO 9001 certification).~~

5. The Agreement is amended to add Sections 9.7, 9.8, and 9.9, and to renumber the sections titled "Injunctive Relief" and "Survival" as Sections 9.10 and 9.11, respectively, as follows (bold/underlining omitted):

9.7 Managed Services; Professional Services; Third-Party Vendors. Provider shall immediately notify County of any terminations or separations of Provider’s employees who performed Services to County under the Agreement or who had access to County data, and Provider must ensure such employees’ access to County data and network is promptly disabled. Provider must ensure all Vendor’s employees with access to County’s network via an Active Directory account comply with all applicable County policies and procedures when accessing County’s network. Provider shall provide privacy and information security training to its employees with access the County’s network upon hire and at least once annually. If any unauthorized party is successful in accessing any information technology component related to Provider, including but not limited to servers or fail-over servers where County data or files exist or are housed, Provider shall report to County within twenty-four (24) hours of becoming aware of such breach. Provider shall provide County with a detailed incident report within five (5) days after the breach, including remedial measures instituted and any law enforcement involvement. Provider shall fully cooperate with County on incident response, forensics, and investigations into Provider's infrastructure as it relates to any County data or County applications. Provider shall not release County data or copies of County data without the advance written consent of County.

9.8 Software Installed in County's Network. Provider shall advise County of any third-party software (e.g., Java, Adobe Reader/Flash, Silverlight) required to be installed and all versions supported. Provider shall support updates for critical vulnerabilities discovered in applicable third-party software. Provider shall 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. Provider must develop and maintain the Software to operate on County-supported and approved operating systems and firmware versions. Provider must mitigate critical or high risk vulnerabilities to the Provider Platform as defined by Common Vulnerability and Exposures (CVE) scoring system within 30 days of patch release. If Provider is unable to apply a patch to remedy the vulnerability, Provider must notify County of proposed mitigation steps to be taken and timeline for resolution. Provider shall ensure the Software provides for role-based access controls and runs with least privilege access. Provider shall support electronic delivery of digitally signed upgrades from Provider's or the third-party licensor's website. Provider shall enable auditing by default in software for any privileged access or changes. The Software must not be within three (3) years from Software's end of life date and the Software must run as least privilege without using fixed or default passwords. Provider shall regularly provide County with end-of-life-schedules for all applicable Software. Provider will 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. Provider will use transport layer security (TLS) 1.1 or current industry standards, whichever is higher, for data in motion.

9.9 Equipment Leased or Purchased from Provider. Provider shall ensure that physical security features to prevent tampering are included in any Equipment provided under this Agreement. Provider shall ensure, at a minimum, industry-standard security measures are followed during the manufacture of the Equipment provided under this Agreement. Any Equipment provided under this Agreement shall not contain any embedded remote control features unless approved in writing by County's Contract Administrator. Provider shall disclose any default accounts or backdoors that exist for access to County's network. If a new critical or high security vulnerability is identified, Provider shall supply a patch, firmware update, or workaround approved in writing by County's Contract Administrator within thirty (30) days after identification of vulnerability and shall notify County of proposed mitigation steps taken. Provider must develop and maintain hardware to interface with County-supported and approved operating systems and firmware versions. If a Provider shall make available, upon County's request, any required certifications as may be applicable per compliance and regulatory requirements (e.g., Common Criteria, Federal Information Processing Standard 140). The Equipment must not be within three (3) years from Equipment's end of life date. Provider shall regularly provide County with end-of-life-schedules for all applicable Equipment. Provider shall support electronic delivery of digitally signed upgrades of any applicable Equipment firmware from Provider's or the original equipment manufacturer's website.

9.10 Injunctive Relief. The Parties represent and agree that neither damages nor any other legal remedy is adequate to remedy any breach of this article, and that the injured party shall therefore be entitled to injunctive relief to restrain or remedy any breach or threatened breach.

9.11 Survival. The obligations under this Article 9 shall survive the termination of this Agreement or of any license granted under this Agreement.

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

7. 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.)

Exhibit 2

IN WITNESS WHEREOF, the Parties hereto have made and executed this First Amendment: 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 _______, 2019, and MISSION CRITICAL SYSTEMS, INC., 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 _____________, 2019

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_____________ 4-10-19
Neil Sharma (Date)
Assistant County Attorney

By_____________ 4/10/19
René D. Harrod (Date)
Deputy County Attorney

NS/RDH
03/20/2019
Mission Critical Systems, Inc. First Amendment
#411834.1

FIRST AMENDMENT TO SYSTEM AND SERVICES AGREEMENT BETWEEN BROWARD COUNTY AND MISSION CRITICAL SYSTEMS, INC.

PROVIDER

WITNESSES:

Signature

STEVEN WALSH
Print Name of Witness

HarrietNewlove
Signature

Harriet Newlove
Print Name of Witness

Mission Critical Systems, Inc.

By
Authorized Signor

Susan Crabtree, President
Print Name and Title

4th day of April, 2019

ATTEST:

-DIRECTOR OF FINANCE
Corporate Secretary or authorized agent

(CORPORATE SEAL)