ADDENDUM # 006

Solicitation Number: ITN #15-FDC-113

Solicitation Title: Comprehensive Healthcare Services - Medical and Hospital Operations at the Reception and Medical Center (RMC)

Opening Date/Time: August 11, 2016 at 3:00 p.m. (Eastern Time)

Addendum Number: Six (6)

Failure to file a protest within the time prescribed in Section 120.57(3), Florida Statutes, or failure to post the bond or other security required by law within the time allowed for filing a bond shall constitute a waiver of proceedings under Chapter 120, Florida Statutes

Please be advised that the changes below are applicable to the original specifications of the above referenced solicitation. Added or new language to the ITN is highlighted in **yellow** below, while language that is deleted is stricken through below.

This Addendum includes the Department's answers to written questions received.

This Addendum also includes the following revisions:

Change No. 1
A change to the Timeline.

TIMELINE
ITN# 15-FDC-113

EVENT	DUE DATE	LOCATION
Release of ITN	December 18, 2015	Vendor Bid System (VBS): http://vbs.dms.state.fl.us/vbs/main_menu
Mandatory Pre-Bid Conference and Site Visit	January 21, 2016 at 10:00 a.m., Eastern Time	Florida Department of Corrections Reception and Medical Center (RMC) 7765 S County Road 231 Lake Butler, FL 32054
First Round of Questions Due	March 10, 2016 Prior to 5:00 p.m., Eastern Time	Submit to: Florida Department of Corrections Bureau of Support Services Email: purchasing@mail.dc.state.fl.us *(reference solicitation number in subject line)*
Anticipated Posting of Answers to First Round of Submitted Questions	April 26, 2016	Vendor Bid System (VBS): http://vbs.dms.state.fl.us/vbs/main_menu

Second Round of Questions Due	May 10, 2016 Prior to 5:00 p.m., Eastern Time	Submit to: Florida Department of Corrections Bureau of Support Services Email: purchasing@mail.dc.state.fl.us (reference solicitation number in subject line)
Anticipated Posting of Answers to Second Round of Submitted Questions	June 7, 2016	Vendor Bid System (VBS): http://vbs.dms.state.fl.us/vbs/main_menu
Sealed Replies Due and Opened	August 11, 2016 ~~July 19, 2016~~ by 3:00 p.m., Eastern Time	Florida Department of Corrections Bureau of Support Services 501 South Calhoun Street Tallahassee, Florida 32399
Evaluation Team Meeting	September 8, 2016 ~~August 2, 2016~~ at 10:00 a.m., Eastern Time	Florida Department of Corrections Bureau of Support Services 501 South Calhoun Street Tallahassee, Florida 32399
Anticipated posting of Respondents initially invited for Negotiations	November 14, 2016 ~~September 26, 2016~~	Vendor Bid System (VBS): http://vbs.dms.state.fl.us/vbs/main_menu
Anticipated Negotiations	December, 2016-March, 2017 ~~October, 2016 – February, 2017~~	Florida Department of Corrections Bureau of Support Services 501 South Calhoun Street Tallahassee, Florida 32399
Best and Final Offers (BAFOs) Due	April 6, 2017 ~~March 23, 2017~~	Florida Department of Corrections Bureau of Support Services 501 South Calhoun Street Tallahassee, Florida 32399
Negotiation Team Meeting	April 20, 2017 ~~April 12, 2017~~ at 2:00 p.m., Eastern Time	Florida Department of Corrections Bureau of Support Services 501 South Calhoun Street Tallahassee, Florida 32399
Anticipated Posting of Intent to Award	July, 2017	Vendor Bid System (VBS): http://vbs.dms.state.fl.us/vbs/main_menu

Change No. 2
A change to Section 2.7, Pricing Methodology to clarify the requested pricing model.

2.7 Pricing Methodology

The Department is seeking pricing that will provide the best value to the State; therefore, interested Vendors must submit a Cost Reply, utilizing the Price Information Sheet, Attachment IV. Vendors are encouraged to submit a Cost Reply in such a manner as to offer the most cost effective, and innovative, solution for services and resources, as cost efficiency for the State will be a consideration in determining best value. Vendors must provide the Cost Reply in accordance with the instructions in Section~~s~~ 4.9~~4.6 and 4.7~~.

The successful Vendor will be responsible for all costs associated with the provision of comprehensive institutional medical and hospital services at the Reception and Medical Center, including costs for non-formulary pharmaceuticals, supplies, instruments, laboratory fees, equipment, and waste disposal (hazardous and non-hazardous). The Vendor must provide adequate equipment and supplies to maintain a fully functional hospital at all times.

Vendors shall provide a single capitation rate, (per-inmate, and per-day) for the delivery of comprehensive institutional medical and hospital services. The Contract payment(s) will be based on the average monthly number of incarcerated inmates as reported in the Department's official Monthly Average Daily Population (ADP) report. To ensure the Department obtains services at the best value, the Department reserves the right, during the Negotiation phase, to consider alternate pricing models, such as cost reimbursement.

Deductions from the monthly payment to the Vendor will be made for salary and travel costs for the Health Services Contract Monitors, approximately $200,000.

Change No. 3
A change to Section 4.9, TAB G to clarify the improvements or cost savings that can be proposed to the Department.

TAB G Additional ideas for improvement or cost reduction, and other supplemental materials - (limit 35 pages)

In **TAB G** of its reply to the ITN, the Respondent is invited to elaborate on additional ideas, pricing structures, or tools for service improvements that are not specifically addressed in **TABs B – F** of its Reply but may be made available via Respondent's offering. The Department is interested in ideas or tools the Respondent believes will provide for greater performance and efficiency of operations. Additionally, Respondents are encouraged to submit alternate pricing structures and the potential cost reductions or benefits to the Department that each would bring; however, actual pricing should only be provided using Attachment IV, Price Information Sheet. Cost points will be awarded based on Attachment IV, as described in Section 4.10 of the ITN. If the Department may request Respondent's submit alternate pricing during the Negotiation Phase, per Section 2.7. Respondent shall make sure to describe in detail

all additional features, capabilities, or services that it will provide in the additional features section.

Change No. 4

A change to Section 3.10 to change the networking and information technology requirements:

~~**3.10 Information Technology Requirements**~~

~~The Contractor must have an automated, integrated tracking and reporting system. The Contractor must provide all computer equipment where needed, technical, and clerical support necessary to support the automated, integrated tracking and reporting system.~~

3.10.1 Corporate Access to the Department's Network

Any access to the Departments network from an outside non-law enforcement entity must be done via a Virtual Private Network (VPN) or via Virtual Local Area Network (VLAN).The Department will require a copy of the Contractor's security policies and a network diagram. After review by the Departments network staff, Information Security staff, the Chief Information Officer will make the final decision on granting access. Access methods may include ~~LAN to LAN or and/or Client VPN~~ a VLAN that exists inside the Department's network, or, a site-to-site VPN, as determined by the Department. The Department may incur costs associated with the access methods to the Contractor in which case the Department may pass that cost on to the Contractor. ~~The contractor will be directly responsible for any costs associated with LAN to LAN connections (e.g. circuit costs) and/or responsible for reimbursement to the Department for fees associated with Client VPN connectivity. Client VPNThe~~ Department may establish ~~connectivity~~ network connectivity fees which, if assessed, ~~are estimated to be approximately $8.00 per user per month and~~ will be reimbursed ~~ment~~ to the Department's Office of Information Technology to cover network costs associated with hardware, data circuits, support, licensing, and maintenance fees. ~~VPN licensing and maintenance fees.~~

3.10.2 VPN Connections

Authorized VPN connections must adhere to the FBI CJIS Security Policy and HIPAA protections standards where applicable and must otherwise support industry best practice.~~, and be provided and managed (including software provision and configuration, and connection support) by a Department-approved VPN service provider.~~ The Contractor requesting or using these connections are financially responsible for all required or related equipment and must adhere to all VPN service provider policies and procedures as well as Department procedures. The VPN service provider will coordinate with the Contractor in determining whether to use the Contractor's equipment to terminate that end of the VPN connection or provide the necessary equipment.

When VPN access is requested the requestor must also present an accurate and complete description of the requestor's information network, including all permanent and temporary remote connections made from and to the requestor's network (required for CJIS compliance), for Department review. Any access or connection to the Department's network, not approved by the FDC Office of Information Technology's (OIT) Chief Information Officer (CIO) or designee, ~~the Department~~ is strictly prohibited.

Contractor workstations accessing the Department's information network via a VPN must operate a fully vendor supported Windows-only operating system that is approved by the Department and protected by all security measures/mitigations required by the CJIS Security policy in effect.

Contractor workstations accessing the Department's information network via a VPN must operate with password protected screen savers enabled and configured for no more than 15 minutes of inactivity

It is the responsibility of the authorized users with VPN privileges to ensure the confidentiality of their credentials and that unauthorized persons are not allowed access to the Department's network by way of these same privileges. At no time shall ~~should~~ any authorized user provide their userID or password to anyone, including supervisors and family members. All users are responsible for the communications and activities conducted by their workstations through the VPN connection to the Department.

Any attempt to fraudulently access, test, measure or operate unapproved software on the Department's network is strictly prohibited. The use of any software capable of capturing information network packets for display or any other use is prohibited without the express consent of the Department's Office of Information Technology.

3.10.3 Contractor ~~Outside Entity~~ Obligations

It is the ~~outside entities'~~ Contractor's and their workforce members' responsibility to maintain knowledge of and compliance with relevant and applicable Department procedures.

Notice of planned events in an outside entity's computing environment that may impact its secured connection, in any way or at any severity level, to the Department must be submitted to the Department at least one week in advance of the event.

The Department must receive notice in electronic and written form from an outside entity when any unexpected event of interest occurs in any way or at any level of severity within or around the outside entity's computing environment that may impact the Department's information security. Events including but not limited to malware (virus, trojan, etc.) discovery, network or system breaches, privileged account compromise, employee or workforce member misconduct are examples of events of interest to the Department.

The Contractor's responsibility for any required equipment includes, but is not limited to currency of configuration, maintenance, support, upgrade, replacement, and other requirements specified in this contract.

The Contractor agrees that all network traffic will be filtered to exclude inappropriate content (e.g. pornographic content), personal identifiable information, any content the Department deems confidential, and be in compliance with all federal and state of Florida laws.

~~Outside entity~~ Contractor workstations are not to access any resource or download any software from the Department's information network without prior approval of the Department.

The Contractor will not grant local administrative privileges to its workforce members or subcontractors.

The Contractor shall conform to applicable information security processes defined and referenced in Department procedures, including, but not limited to, FDC Procedure 206.010, Information Technology Security relating to HIPAA.

Before connection, and while connected to a VPN formed with the Department, the ~~outside entity's~~ Contractor's computing environment (computing devices including workstations, servers, and networking devices) must be operating the latest available software versions and applicable patches, and have the following implemented with supporting policies or procedures available for review by the Department:

- Active and effective network device, server and workstation operating system and layered software patch or update processes
- Department approved, up-to-date server and workstation anti-virus/malware software (all components) installed with active and effective patch or update processes in place

The Contractor will not introduce any workload on the Department's network, including video conference, telemedicine, Software-as-a-Service (SaaS) systems, video streaming, and training curriculum without the written approval of the Department. Contractor workforce members with network ~~VPN~~ access privileges to the Department's network shall not use non-Department email accounts (i.e., Hotmail, Yahoo, Gmail, AOL, or similar), or other external information resources to conduct personal or Department business, except under the conditions as specifically approved by the Department. ~~ensuring a reduced risk to Department data and that Department business is never confused with personal business.~~

With regard to VPN connections used by ~~outside entities~~ the Contractor that are provided by Department-approved VPN providers, the Department bears no responsibility if the installation of VPN software, or the use of any remote access systems, causes system lockups, crashes or complete or partial data loss on any outside entity computing or network equipment.

The ~~outside entities~~ the Contractor is solely responsible for protecting (backing up) all data present on its computing and network equipment and compliance with all regulatory legislation. In addition, Contractor employees must adhere to all Department policies regarding data retention and destruction protocols. No data destruction shall occur unless written authorization by the Department is granted. Further, if local file storage is necessary at any institution then the Contractor will use a network share for file storage that has been provisioned to the Contractor.

3.10.4 Contractor's Computer & Network Environment

The Contractor will not be allowed to install, create, or use their own network, including Local Area Network (LAN), Wide Area Network (WAN), Wireless Local Area Network (WLAN), or cellular networks for any reason, unless approved in writing by the Department.

~~In addition to the Contractor providing their own data network and connectivity devices, all associated IT hardware~~ All computer workstations and network-connected medical devices for use at any ~~the~~ local correctional facility ~~level~~ will be provided by and maintained by the Contractor. This includes, but is not all inclusive, hardware such as personal computers and laptops (including software licenses), tablet PC's, thin clients, printers, fax machines, scanners, and video conferencing (if approved). The Contractor may not install managed or unmanaged switches onto the Department's network without approval from the Department. ~~switches, and UPS for switches.~~

Use of mobile devices, whether work issued or personal, will not be allowed without the written approval of the Department. In the event of such an approval a business justification must be submitted in writing along with a clear demonstration that the mobile devices fall within the Criminal Justice Information Systems (CJIS) Security Policy and be centrally managed by a mobile device management (MDM) solution.

3.10.5 Transmitting Health Information via Email

In conducting its mission the Department is required to communicate with parties outside of its internal email and information systems. These communications may include electronic protected health information (ePHI) or other confidential information governed by any of the Health Insurance Portability and Accountability Act (HIPAA), The Health Information Technology for Economic and Clinical Health **(**HITECH**)** Act or Chapter ~~71-A~~ 74-2, F.A.C These and other regulations require that electronic transmission of ePHI or confidential information be encrypted.

The current practice requires passing health or other confidential information by way of phone calls, faxing, encrypted electronic mail, and traditional paper mail.

If the Contractor requires using email to transport ePHI or other confidential health information, it must establish and host an email encryption solution. The solution must be approved by the Department's Office of Information Technology (OIT) and meet or exceed all federal and state regulations, including those mentioned above before implementation.

The Department reserves the right to implement email security for all types of devices, and the Contractor will comply with using these security requirements as dictated in the future.

3.10.6 Contractor Data Availability

The Contractor shall have the capability for the Department to send data to and pull data from the Contractor's provided health service information technology systems via a secure transport method (SFTP, Secure Web Services, etc.); furthermore, the data format should either be XML-based or delimiter-separated values. It is the Contractor's responsibility to provide all necessary documentation to assist in the integration of data which includes but is not limited to crosswalk tables for code values, schemas, and encodings.

The Contractor and their staff will be held to contractual obligations of confidentiality, integrity, and availability in the handling and transmission of any Department information.

1. No disclosure or destruction of any Department data can occur without prior express consent from the Department's Office of Information Technology and Contract Manager.

2. The Contractor shall timely return any and/or all Department information in a format acceptable to the Department when the contractual relationship effectively terminates, not to exceed 10 business days.

3. The Contractor shall provide certification of its destruction of all Departmental data in its possession, in accordance with NIST Special Publication 800-88 when the need for the Contractor's custody of the data no longer exists.

4. The Contractor must maintain support for its services following an emergency that affects the facilities and systems it maintains or those maintained by the Department. Following an emergency that affects the Contractor's facilities or production systems, the Contractor must provide access and use of a backup system with the same functionality and data as its operational system within twenty-four (24) hours. The Contractor must also guarantee the availability of data in its custody to the Department within twenty-four (24) hours following an emergency that may occur within the Contractor's facilities or systems. Following an emergency that affects the Department's facilities or systems, the Contractor must continue to provide access and use of its production systems once the Department has recovered or re-located its service delivery operations.

5. The introduction of wireless devices at facilities is subject to prior review and approval by the Contract Manager and the Department's Office of Information Technology and Contract Manager. The Contractor is responsible for notifying the Department before introducing wireless devices into facilities.

3.10.7 Information Security Auditing and Accountability

The Contractor will provide the Department audit and accountability controls to increase the probability of authorized system administrators conforming to a prescribed pattern of behavior. The Contractor in concert with the Department shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability including servers, mainframe, firewalls, routers, switches.

Events to be audited must include those required in the CJIS Security Policy, including but not limited to any audit or logging events mentioned in this document.

3.10.8 Auditable Events and Content (Servers, Mainframes, Firewalls, Routers, Switches)

The Contractor shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The Department shall specify which information system components carry

out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The Contractor shall produce and maintain for the required periods, at the system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The Department shall periodically review and update the list of auditable events.

3.10.9 Events

Events to be logged and audited include those required in the CJIS Security Policy, including but not limited to:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

The Contractor must monitor security logs for suspicious behavior and self-audit for these controls. The Department reserves the right to ask for reports relating to these controls and self-audits. The Contractor shall provide log sources for forwarding and aggregation in the Department's Security Information and Event Management (SEIM) system upon request.

3.10.10 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type and description of event
4. User/subject identity.
5. Outcome (success or failure) of the event.

3.10.11 Response to Audit Processing Failures

The Contractor shall provide alerts to the Department's CIO or designee in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

3.10.12 Time Stamps

The Contractor shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

3.10.13 Protection of Audit Information

The Contractor shall protect audit information and audit tools from modification, deletion and unauthorized access.

3.10.14 Audit Record Retention

The Contractor shall retain audit records for at least 365 days. Once the minimum retention time period has passed, the Contractor shall continue to retain audit records until the Department determines they are no longer needed for administrative, legal, audit, or other operational purposes. The Contractor should request written approval from the Department prior to destruction of audit records.

3.10.15 Compliance Requirements

The Contractor must comply with all applicable State and Federal security requirements including HIPAA, the FBI CJIS Security Policy, and Chapter ~~71A-1~~ 74-2, F.A.C, and all applicable Department information security policies. ~~, *Florida Information Technology Resource Security Policies and Standards*.~~

So as to be compliant with the Health Insurance Portability and Accountability Act (HIPAA), any service, software, or process to be acquired by or used on behalf of the Department that handles and/or transmits electronic protected health information must do so in full HIPAA compliance and with encryption provided as a part of the service, software, or process. In addition, the transmission and encryption scheme supplied by the Contractor must be approved by the Department prior to acquisition.

Any service, software, or process used in service to the Department that includes a userID and password component must ensure said component includes at a minimum capabilities for password expiration and confidentiality, logging of all UserID activities, lockout on failed password entry, provisions for different levels of access by its userIDs, and intended disablement of userIDs and be evidenced as such by the Contractor's own security policies and Active Directory (AD) group policy settings.

Any and all introductions or subsequent changes to information technology or related services provided by the Contractor in the Department's corrections environment must be communicated to and approved by the Department prior to their introduction. As examples, the implementation of wireless (Bluetooth, 802.11, cellular, etc.) technology or use of USB based portable technology.

The Contractor must comply with Department procedures that relate to the protection of the Department's data and its collective information security which include but are not limited to Procedure 206.007, *User Security for Information Systems Office of Information Technology*

Internal Remote Access; and the Contractor, its subcontractors, and their staff will be held to contractual obligations of confidentiality, integrity, and availability in the handling and transmission of any Department information.

~~Any and all information security technology or related services (e.g. internet monitoring software) in the Department's corrections environment are to be provided by the Contractor unless the lack of these technologies and services is approved by the Department and Office of Information Technology.~~

The Department will maintain administrative and management control over any aspect of ~~this~~the services provided by the Contractor which govern criminal justice information within its corrections environment to the degree necessary to maintain compliance with the U. S. Department of Justice Information Services Security Policy. Subsequently, a separate Management Control Agreement (MCA) must be executed between the Contractor and Department.

The Contractor must agree to comply to any applicable requirement necessary to the Department's compliance with local, state, and federal code or law.

All Contractors must be able to comply with Department procedures that relate to the protection (maintaining confidentiality, integrity, and availability) of the Department's data and its collective information security. Access to Department information resources will require use of the Department's security access request application (SAR), or similar process, when applicable.

The Contractor must recognize the Department's entitlement to all Department provided information or any information related to the Department generated as a result of or in participation with this service.

No disclosure or destruction of any Department data by the Contractor or its contracted parties can occur without prior express consent from a duly authorized Department representative.

The Contractor must provide for the timely and complete delivery of all Department information in an appropriate and acceptable format before the contractual relationship effectively terminates.

The Contractor must provide certification of its destruction of all of the Department's data in accordance with NIST Special Publication 800-88, Guidelines for Media Sanitation, when the need for the Contractor's custody of the data no longer exists.

The Department's data and contracted services must be protected from environmental threats (Contractor's installation should have data center controls that include the timely, accurate, complete, and secure backup (use of offsite storage) of all Department information, and other controls that manage risks from fire, water/humidity, temperature, contamination (unwanted foreign material, etc.), wind, unauthorized entry or access, theft, etc.).

The Contractor should be prepared to guarantee availability of Department data and its service during a disaster regardless of which party is affected by the disaster.

Correctional institutions site plans and plan components (electrical, plumbing, etc.) are exempt from public record and must be kept confidential.

If applicable, the Contractor shall supply all equipment necessary to provide services outlined in this solicitation. Any Contractor equipment that ~~will not~~ requires connection to the Department's information network must be reviewed and approved by the Department's Contract Manager and CIO.

If applicable, the Contractor will host the Department's information and/or services provided in a data center protected by appropriate industry best practice security measures/mitigations, including but not limited to, the following:

1. Controlled access procedures for physical access to the data center;
2. Controlled access procedures for electronic connections to the Contractor's network;
3. A process designed to control and monitor outside agencies and other contractors' access to the Contractor's information network;
4. A Firewalling device;
5. Server based antivirus/malware software;
6. Client based antivirus/malware software;
7. Use of unique userIDs with expiring passwords;
8. A process that involves collection of userID activities and regular review of these activities for unauthorized access or privileges; and
9. A process that ensures up to date software patches and up to date malware signature files are applied to all information resources.
10. Comply with the most recently published version of the CJIS Security Policy.

The Contractor shall maintain an Information Security Awareness program. This program will be designed to keep users knowledgeable on information security best practices and current threats to the Contractor's resources.

The Contractor's solution and services must operate to the Department's satisfaction on its ~~current~~ standard personal computer platform (which is subject to change), if applicable, which currently is configured with:

- Intel Core I5-4590 Processor (Quad Core, 3.30 GHz Turbo, 6MB Cache, with HD Graphics 4600
- 8 GB RAM
- 500 GB 7200 RPM Hard Drive
- 16X DVD-ROM RW
- 10/100/1000 Mb NIC
- Onboard or External Graphics Card
- Keyboard
- Mouse
- Window 7 Operating System
- Office 2007 (in transition to O365)
- Trend Micro Anti-virus
- Internet Explorer 11

- Mocha TN3270 version 1.8
- Java 1.8.0_51
- Adobe Flash Player version 19