Request for Quote (RFQ)
RFQ-19-014
Virtual Desktop Infrastructure (VDI) Platform

1. Overview

The purpose of the Virtual Desktop Infrastructure (VDI) Platform is to purchase and deploy a virtual desktop platform, and re-purpose 7,000 existing desktops as thin clients. In addition to the purchase of hardware and software, the Department will purchase professional services to include project management, analysis, design, planning, configuration, implementation, and continued support for the complete VDI Platform.

The Department's current environment includes 50 separate locations, with circuits ranging from 10-45 megabits per second (mbps). The Correctional Institution (CI) and Annex locations with desktop totals and circuit speeds are included in Attachment I, Department Enterprise Locations. More than half of the desktops are represented by the specifications below:

- Dell OptiPlex 5040 with Intel i5-6500 CPU, 8GB RAM, 450GB HD
- Dell OptiPlex 7020 with Intel i5-4590 CPU, 4GB RAM, 450Gb, HD
- Dell OptiPlex 380 with Intel Dual Core E5300 CPU, 2GB RAM, 150GB HD

1.1. Background and Purpose

Section 945.025, Florida Statutes (F.S.), gives the Florida Department of Corrections (Department) responsibility for the supervision, protective care, custody, and control of the buildings, grounds, property, and all other matters pertaining to facilities and programs for the imprisonment, correction, and rehabilitation of adult inmates and offenders. The Department is the third (3rd) largest state prison system in the country, with approximately 97,000 inmates and nearly 167,000 offenders on active community supervision. The Department has 144 facilities statewide, including: 50 major institutions, 17 institutional annexes, 35 work camps, two (2) road prisons, one (1) forestry camp, one (1) basic training camp, 16 contracted community release centers, 12 Department-operated community release centers, three (3) re-entry centers, and seven (7) private prisons (operated by the Florida Department of Management Services (DMS).

The Department's Office of Information Technology (OIT), is the organizational unit within the Department that's responsible for information technology infrastructure, issues, and resources.

The Department is seeking qualified, cooperative purchasing Vendors, on GSA Schedule 70 for the provision and implementation of a turn-key Virtual Desktop Infrastructure (VDI) Platform, enabling 7,000 Department end-points to concurrently access a virtual Microsoft Windows 10 Enterprise desktop solution using DMS-approved Alternate Contract Source (ACS) 252-GSA.

The Department intends to award one (1) statewide Contract, to a single Vendor, for the provision of services. However, the Department reserves the right to purchase hardware and/or software from separate Vendor(s).

1.2. Service Implementation

The Vendor must have the capacity to begin service delivery, as described in this RFQ, no later than December 1, 2018. The solution must be fully implemented by May 31, 2019.

1.3. Term

As a result of the RFQ, the successful Vendor will be awarded a Contract, with the initial term of five (5) years. If hardware and/or software is purchased separately, it would be completed through an MFMP Purchase Order (PO).

1.4. Contract Renewal

The Department may renew the resulting Contract for up to five (5) years, or portions thereof, in accordance with Section 287.057(13), F.S., at the same prices, terms, and conditions. If the Department makes the determination to renew a resulting Contract, it will provide written notice to the Vendor no later than 90 days prior to the Contract expiration date.

1.5. Instructions to Respondents

All responses to this RFQ should be sent to purchasing@fdc.myflorida.com by 5:00 p.m., Eastern Time, on October 2, 2018.

Any questions that may arise related to this RFQ should be directed, in writing, to Tammy Davis at purchasing@fdc.myflorida.com.

1.6. Basis of Award

Contract award(s) will be made to the GSA Schedule 70 Vendor(s) providing the best value to the State, based upon each Vendor's ability to meet the Department's requirements (as evidenced by their submitted Quote), funding availability, and the Department's determination of service and equipment needs.

1.7. Definitions

The terms used in this RFQ, unless the context otherwise clearly requires a different construction and interpretation, have the following meanings:

1) **Breach of Contract:** A failure of the Vendor(s) to perform in accordance with the terms and conditions of the resultant Contract.

2) **Contract:** The agreement between the successful Vendor and the Department resulting from this RFQ, including a Purchase Order that may be issued by the Department to the successful Vendor.

3) **Contract Non-Compliance**: Failure to meet or comply with any requirement or term of the resultant Contract.

4) **Corrective Action Plan (CAP):** A Vendor's written comprehensive plan to remedy deficiencies discovered in the course of Contract monitoring and/or discovered at any time during the term of the Contract.

5) **Day:** Calendar day, unless otherwise stated.

6) **Deliverables:** Those services, items, and/or materials provided, prepared and delivered to the Department in the course of Contract performance. Deliverables are specifically described in Section 2.16 of this RFQ.

7) **Department:** The Florida Department of Corrections (FDC).

8) **Evaluation Methodology:** The process utilized by the Department to evaluate the Quotes received from qualified Vendors.

9) **General Services Administration (GSA) Cooperative Purchasing Schedule 70:** GSA schedules allow the government to contract with commercial companies for the provision of goods and services at volume discount pricing. The "Cooperative Purchasing" distinction is required to authorize State and local government entities eligibility to access to Schedule 70. The Department is authorized to purchase under GSA Schedule 70 through a DMS-approved ACS, 252-GSA.

10) **HIPAA:** The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) requires the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. The awarded Vendor shall comply with HIPAA, 1996 (42 U.S.C. 1320d-1329d-8), and all applicable regulations promulgated thereunder.

11) **Prison Rape Elimination Act (PREA):** Where used herein, refers to Part 115 of Title 28 C.F.R., National Standards to Prevent, Detect, and Respond to Prison Rape, under the "Prison Rape Elimination Act of 2003." The Act provides for analysis of the incidence and effects of prison rape in federal, state, and local institutions, and for information, resources, recommendations, and funding to protect individuals from prison rape.

12) **Responsible Vendor:** A Vendor who has the capability in all respects to fully perform the Contract requirements, and the integrity and reliability that will assure good faith performance.

13) **Subcontract:** An agreement entered into by the Vendor with any other person or organization that agrees to perform any performance obligation for the Vendor specifically related to securing or fulfilling the Vendor's obligations to the Department under the terms of the resultant Contract.

14) **Value-Added Services**: Additional services the Vendor may offer to provide to the Department, above meet the minimum services requirements and specifications of this RFQ, offered at no additional cost to the Department.

15) **Vendor or Respondent:** A legally qualified corporation, partnership or other entity authorized to conduct business on GSA Schedule 70 and with the State of Florida submitting a response to the Department, pursuant to this RFQ.

2. Scope of Work

This section contains the Scope of Work that will be required in any Contract(s) resulting from this RFQ. All services to be performed by, or under the direction of the Vendor under any resultant Contract, shall meet or exceed the minimum requirements outlined in this RFQ.

2.1. Scope of Services

2.1.1. Project Goals

(a) Purchase a turn-key Virtual Desktop Infrastructure (VDI) Platform.
(b) Receive an expert recommendation from the Vendor for application deployment and re-purposing the existing desktops as thin client endpoints.
(c) Re-purpose existing desktops as thin clients.
(d) Migrate 7,000 end-points to a virtual Windows 10 Enterprise desktop.

The Vendor shall deliver a turn-key Virtual Desktop Infrastructure (VDI) Platform allowing up to 7,000 end-points to concurrently access a virtual Windows 10 Enterprise desktop. The Vendor's response shall include all costs for hardware, software, project management, and professional services to analyze, design, plan, configure, implement, and support the VDI Platform.

All hardware, software, and other components of the solution shall become property of the Department upon completion of the implementation and shall be hosted centrally in the state datacenter. The existing virtual infrastructure and hardware resources of the State datacenter shall not be utilized in this solution. The Vendor's response shall include all server hardware and software required to meet the requirements of this RFQ. The State datacenter shall be used for co-locating the VDI solution. Co-location shall include floor space, Ethernet connectivity, and electrical power.

No server hardware shall be required at remote sites. The Department's users will access the virtual desktop from multiple remote locations across the state, which are all connected by the MyFloridaNet (MFN) network.

The solution shall integrate with the Department's Microsoft Active Directory and other industry standard third-party management tools. Access to the platform shall be limited to approved users and devices as set forth by the Department during the project planning.

The Vendor shall be responsible for ongoing maintenance and support of the VDI platform hardware and software components. The Department will work with the Vendor for future endpoint operating system updates or modifications to endpoint images.

The awarded Vendor will evaluate the user needs through analysis and prepare a deployment design and implementation plan.

2.2. Department Responsibilities

The Department is responsible for assisting the Vendor by providing Department-specific information necessary for the Vendor to analyze, design, plan, configure, implement, and support the VDI Platform. The Department will also:

(a) Configure the MFN network circuits.
(b) Perform on-site work related to the local endpoint configurations.
(c) Migrate user data from local servers to central datacenter servers in coordination with the implementation.
(d) Make decision on implementation and rollout options after consideration of Vendor's recommendation for VDI application deployment and repurposing the desktops.

2.3. Vendor Requirements

The Vendor is responsible for the full configuration and installation of the solution in the State datacenter, leading the pilot planning and testing, training the Department's system administrators, and providing ongoing support of the platform. The Vendor will also conduct the pilot testing, remediation, and documentation of end-point deployment procedures, to fully prepare the Department staff for on-site work. Prior to implementation, the Vendor will demonstrate load testing to simulate a full 7,000 concurrent connections on the VDI Platform and for bandwidth validation, the load testing will be performed on pilot sites.

The Vendor shall include the following information in its Response:

(a) Provide a complete project implementation schedule along with the approach to implement the proposed solution with minimal impact to staff operations. Include a pilot phase for four (4) sites up to 100 users at each location. The Vendor shall be responsible for creating three (3) "golden images" and configuring them for staff use. Training from the Vendor shall include topics to create and modify images, migrate additional users to the VDI Platform, and general system administration.
(b) Provide validation that the proposed VDI Platform is consistent with the guidelines or requirements set forth by each manufacturer of the hardware and software components used in this VDI solution.
(c) Provide a detailed checklist of high-level configuration steps that will be necessary for this engagement.
(d) Provide high level diagram(s) showing each component of the solution and how they integrate with each other.
(e) Provide in detail the delivery mechanisms for providing the staff a virtual Windows 10 Enterprise desktop with applications required by this RFQ.
(f) Provide a detailed plan on how printing will be handled by the proposed solution. While VDI users will use stationary workstations, staff may move from building to building throughout the day. Additionally, the system should allow access to a local printer if the workstation is configured with one.
(g) Describe how the system will function for both Microsoft Office 365 G3 and K1 licensed users. G3 users will have access to the complete Office Pro Plus desktop application suite, while K1 will use Outlook Web Access with the ability to view attachments online and use Office 2007 within the virtual desktop. Vendors should discuss potential conflicts and offer alternatives in the response.
(h) Describe how your solution integrates with Microsoft Active Directory and any potential integrations with the Department's Cloud Identity Management solution, Centrify.
(i) Provide an operational plan that describes how the solution will be managed once it is installed, including post-implementation support available to the Department. The operational plan shall include RACI chart, test plans for upgrades to the system firmware or software, and Service Level Agreements (SLA) for operations.
(j) Provide an end user device transition plan that includes steps for staff to migrate users to the solution and best practices for long term end user support and troubleshooting
(k) Provide an expert opinion on the Department's staffing resources necessary to adequately provide post-implementation support.
(l) Describe in detail the Vendor's plan for training four Department staff to support the VDI platform.
(m) Provide the details of a high availability design with redundancy limited to a single site. The detail should include a statement of expected uptime and plan to measure uptime.

2.4. Solution Requirements

(a) The Department has 18,000 individual Active Directory accounts. Potentially each of these are candidates for logon to the VDI Solutions; however, the Department's concurrent user license requirement is 7,000 end-point connections.
(b) The solution shall be designed for high availability with redundancy limited to a single site. Network transport and electrical power will not be a factor in calculation of high availability.
(c) The solution shall have an expected life span no less than five (5) years.
(d) The solution shall support ability to add capacity via scale-out or scale-up methods.
(e) The solution shall include in the proposed price, ongoing upgrades to firmware and software.
(f) The solution shall support VDI sessions through the Department virtual private network solution.
(g) The solution shall be configured to use no more than 125 Kbps per user session using basic productivity applications such as Microsoft Office. Specialty application requirements will be discussed with awarded Vendor during the analysis and planning.
(h) The solution shall operate with network latency up to 100 ms Round Trip Time (RTT).
(i) The solution shall support 7,000 concurrent Windows 10 VDI sessions.
(j) The Vendor shall create up to three (3) Windows 10 Enterprise images based on Department requirements.
(k) FDC Applications requirements:
    i. Windows 10 Enterprise desktop;
    ii. Office365 Pro Plus;
    iii. Office 2007 Pro;
    iv. SharePoint 2016 on premise;
    v. Adobe Acrobat Reader;
    vi. Mocha/TN3270 and Bluezone Client;
    vii. Microsoft Edge, Internet Explorer 11, Mozilla Firefox, and Google Chrome for internal web applications;
    viii. TrendMicro Antivirus client if appropriate for the VDI Platform; alternative recommendations should be included in the response;
    ix. SCCM agent if appropriate for the recommended deployment method;
    x. Java and Flash to support third-party web applications such as Kronos Time Keeping; and,
    xi. Hyland OnBase 17 and Kofax 9.0.
(l) FDC Hardware Integration:
    Not all of the devices below will be included in the initial deployment, but the VDI Platform must support these types of devices. The Department intends to work with the awarded Vendor to receive guidance on hardware integration, choose from the recommended options, and prepare the appropriate deployment strategy. The Department's printing environment includes different printer models from HP, Dell, Canon, Brother, and Konica/ Minolta.
    i. USB devices equivalent to Kingston DataTraveler G2 4000, which is FIPS 140-2 compliant;
    ii. USB secure hard drives equivalent to Apricorn Aegis;
    iii. Dell external USB CD/DVD+RW Drives;
    iv. Local scanners;
    v. Axom body camera system;
    vi. Local and network printers;
    vii. Network shares; and,
    viii. Mainframe printing (Custom internal application: "save-a-tree").
(m) Test Environment:
    i. The Department requires a scaled-down test environment to assist with trouble resolution and testing of system changes during the change management process.
    ii. The test environment, whether physical or virtual, shall be a platform for the Department to make changes without affecting the production system.

2.4.1. Reporting Requirements

(a) The solution shall provide system monitoring and be capable of exporting logs to Security Information and Event Management software (SIEM).
(b) The solution shall conform to service level metrics that can be tabulated in numerical form for monitoring and performance measurement.
(c) Alerts and reports shall be developed by the Vendor to inform the Department of service level metrics and performance measurement.

2.4.2. Technical Support Requirements

(a) The Vendor shall provide technical support to the Department for its daily administration, upgrades and repair of the proposed VDI solution.
(b) The Vendor shall provide a single support contact for issue escalation.
(c) The Vendor shall work within the FDC OIT Service Management processes including the formal change management process.

2.4.3. Security Standards

(a) The Vendor shall provide solutions that adhere to Chapter 74-2, Florida Administrative Code (F.A.C.).
(b) The Vendor shall provide solutions that adhere to Attachment VII, Criminal Justice Information System (CJIS) Security Policy, and execute a security addendum to the Contract, which is required for administrative access to systems containing CJIS data. Upon award, the Vendor shall provide certificates to demonstrate compliance.

2.5. Value-Added Services

Value-added services are services that the Vendor offers, for no additional cost to the Department, as part of the resulting Contract, and which clearly exceed the minimum requirements of this RFQ.

Any value-added services offered by the Vendor, if accepted by the Department, might become requirements and be a part of the minimum service specifications contained in the resulting Contract.

2.6. Conduct and Safety Requirements

2.6.1. The Vendor shall ensure that all Vendor's staff adhere to and are provided a copy of these requirements. A signed receipt of acknowledgment shall be maintained in the Vendor's staff's employee personnel file. The Department reserves the right to disqualify, prevent, or remove any staff from any work under the resultant Contract. The Department is under no obligation to inform the Vendor of the criteria for disqualification or removal.

2.6.2. In addition, the Vendor shall ensure all staff adhere to the following requirements:

(a) The Vendor's staff shall not display favoritism to, or preferential treatment of, one offender, or group of offenders, over another.
(b) The Vendor's staff shall not deal with any offender except in a relationship that supports services under any resulting Contract. Specifically, staff members must never accept, for themselves or any member of their family, any personal (tangible or intangible) gift, favor, or service from an offender, or an offender's family or close associate, no matter how trivial the gift or service may seem. The Vendor shall

report any violations or attempted violation of these restrictions to the Department's Contract Manager, or designee. In addition, no staff member shall give any gifts, favors, or services to offenders, members of their family, or close associates.

(c) The Vendor's staff shall not enter into any business relationship with inmates, offenders or their families (example – loans, selling, buying, renting, leasing, or trading personal property), or personally employ offenders, or their families, in any capacity. Unless approved in writing by the Department's Contract Manager, or designee, the Vendor's staff shall not have outside contact (other than incidental contact) with an offender, their family or close associates, except for those activities completed under the resulting Contract.

(d) The Vendor's staff shall not engage in any conduct which is criminal in nature, or which would bring discredit upon the Vendor or the Department. In providing services pursuant to the resulting Contract, the Vendor shall ensure its employees avoid both misconduct and the appearance of misconduct.

(e) Any violation or attempted violation of the restrictions referred to in this section regarding employee conduct shall be reported by phone and in writing to the Department's Contract Manager, or designee, including proposed action to be taken by the Vendor. Any failure to report a violation, or take appropriate disciplinary action against the offending party or parties, shall subject the Vendor to punitive action, up to and including termination of any resulting Contract.

(f) The Vendor shall have a written report of any incident described above, or requiring investigation by the Vendor, to the Department's Contract Manager, or designee, within 24 hours of the Vendor's knowledge of the incident.

2.7. Staff Background/Criminal Records Checks

2.7.1. The Vendor's or any subcontractor's staff assigned to the resulting Contract shall be subject, at the Department's expense, to a Florida Department of Law Enforcement (FDLE) Florida Crime Information Center/National Crime Information Center (FCIC/NCIC) background/criminal records check as required in the Department's Procedure 602.016(10). This background check will be conducted by the Department and may re-occur at any time during the Contract period. The Department has full discretion to require the Vendor to disqualify, prevent, or remove any staff from any work under the resulting Contract. The use of criminal history records and information derived from such records are restricted pursuant to Section 943.054, F.S. The Department shall not disclose any information regarding the records check findings or criteria for disqualification or removal to the Vendor. The Department shall not confirm to the Vendor the existence or nonexistence of any criminal history record information. In order to carry out this records check, the Vendor shall provide, upon request, the following data for any staff or subcontractor's staff assigned to the Contract: Full Name, Race, Gender, Date of Birth, Social Security Number, Driver's License Number and State of Issue.

The Vendor shall ensure that the Department's Contract Manager, or designee, is provided the information needed to have the FCIC/NCIC background check conducted prior to any new staff being assigned to work under the resulting Contract. The Vendor shall not offer employment to any individual, or assign any individual to work under the resulting Contract, who has not had an FCIC/NCIC background check conducted.

2.7.2. When providing contractual program services the Vendor shall obtain a Level II background screening (which includes fingerprinting to be submitted to the Federal Bureau of Investigation (FBI), and results must be submitted to the Department prior to any current or new Vendor's staff being assigned to work under any

resulting Contract. The Vendor shall bear all costs associated with this background screening. The Vendor shall not consider new employees to be on permanent status until a favorable report is received by the Department from the FBI.

2.7.3. No person barred from any FDC institution, or other Department facility, shall provide services under the resulting Contract without prior written approval from the Department's Contract Manager, or designee.

2.7.4. Offenders/Inmates shall be precluded from any supervision or placement at a program where pre-existing or continuous close personal relationships exist between the offender/inmate and any staff of the Vendor. It is the responsibility of the Vendor to advise the Department's Contract Manager, or designee, of any known pre-existing close personal relationships between staff and offender(s). Rule 33-208.002(26), F.A.C. shall apply at the Program, which stipulates that marriage between employee and offender is prohibited.

(a) The Vendor shall immediately report any new arrest, criminal charges, or convictions of a current employee under the resulting Contract.

(b) Note that a felony or first-degree misdemeanor conviction, a plea of guilty or nolo contendere to a felony, or first-degree misdemeanor crime, or adjudication of guilt withheld to a felony or first-degree misdemeanor crime, does not automatically bar the Vendor from hiring the proposed employee. However, the Department reserves the right to prior approval in such cases. Generally, two (2) years with no criminal history is preferred. The Vendor shall require that all proposed employees provide to them the details of any criminal background information. The Vendor shall make full written report to the Department's Contract Manager, or designee, within 24 hours whenever an employee has a criminal charge filed against them, an arrest, or receives a Notice to Appear for violation of any criminal law involving a misdemeanor, or felony, or ordinance (except minor violations for which the fine or bond forfeiture is $200 or less), or when the Vendor or any of their staff has knowledge of any violation of the laws, rules, directives or procedures of the Department.

2.8. Deliverables

The following services or service tasks are identified as deliverables for the purpose of any resultant Contract.

2.8.1. Service requirements, as stated in Section 2, Scope of Work; and
2.8.2. Reports, as required in Section 2.9, General Reporting Requirements.

2.9. General Reporting Requirements

The Vendor shall submit the reports delineated below in an approved format to the Department's Contract Manager, or designee. The Department reserves the right to modify reporting requirements as necessary, upon 30 calendar days' written notification to the Vendor. The Department encourages the Vendor to submit copies of the required reports by email, utilizing Microsoft Office Suite, and/or Adobe applications. All reports shall include the Vendor's name, Contract number, mailing address, email address, phone number, location(s) of program and program title. All reports shall be submitted by the dates delineated below and shall be considered late after that date.

2.9.1. Program Invoice and Monthly Summary Reports

Program Invoices, which shall specify the month being billed, Vendor's name, Contract number, invoice number, federal employer identification number (FEIN), unit rates in accordance with the Price Sheet, and dates of service, shall be submitted to the Department's Contract Manager, or designee, within 10 calendar days following the end of the previous month of service delivery, and shall include program uptime monitoring data. This Monthly Report shall be submitted in a format approved by the Department's Contract Manager, or designee.

2.9.2. Ad-Hoc Reports

The Vendor shall provide the Department ad-hoc reports, upon request of the Department's Contract Manager, or designee, within the timeframe specified in the request.

2.10. Performance Measures and Performance Monitoring

The Department desires to contract with a Vendor who clearly demonstrates its willingness to be held accountable for the achievement of certain performance measures in successfully delivering services under any Contract resulting from this RFQ. Therefore, the Department has developed the following Performance Measures which shall be used to measure the awarded Vendor's performance and delivery of services.

Listed below are the key Performance Expectations, Measures, and Financial Consequences deemed most crucial to the success of the overall desired service delivery. The Vendor shall ensure that the stated performance expectations and standards (level of achievement) are met.

2.10.1. Performance Measure #1 – Availability

Expectation: The Vendor's Virtual Desktop Infrastructure (VDI) Platform shall be configured to support high availability with an uptime equivalent to the uptime set forth in the Vendor's response, once fully implemented.

Measure: Availability will be measured pursuant to the plan provided in the Vendor's response, and monitored monthly following the date of implementation.

Financial Consequence: The Department will impose financial consequences in the amount of $1,000.00 for each tenth of a percentage point less than the expectation of availability during a single month.

2.10.2. Performance Measure #2 – Implementation

Expectation: The Vendor's Virtual Desktop Infrastructure (VDI) Platform shall be configured and fully implemented within four (4) months from the date of Contract execution.

Measure: Time will be reviewed between the date of Contract execution and the day that full implementation is completed.

Financial Consequence: The Department will impose financial consequences in the amount of $1,000.00 per calendar day that the VDI Platform is not fully implemented, as required, by May 31, 2019.

2.10.3. The standard for each performance measure must be met for the amount of time specified. The Vendor shall advise the Department, in writing, of any extenuating or mitigating circumstances that will prohibit them from meeting the above-outlined performance measure standards.

The Vendor expressly agrees to the imposition of financial consequences, in addition to all other remedies available to the Department by law.

The Department's Contract Manager, or designee, will provide written notice to the Vendor's Representative of all financial consequences assessed, accompanied by detail sufficient for justification of assessment. Within 10 calendar days of receipt of a written notice of demand for consequences due, the Vendor shall forward payment to the Department. Payment shall be for the appropriate amount, be made payable to the Department, and be in the form of a cashier's check or money order. As an alternative, the Vendor may issue a credit, for the amount of the financial consequences due, on the next monthly invoice following imposition of consequences; documentation of the amount of consequences imposed shall be included with the invoice.

By execution of any resulting Contract, the awarded Vendor hereby acknowledges and agrees that its performance under the resulting Contract shall meet the standards set forth above. Any failure by the awarded Vendor to achieve the Performance Measures identified above will result in assessment of Financial Consequences. Any such assessment and/or subsequent payment thereof shall not affect the Vendor's obligation to provide services as required by this RFQ.

2.11. Monitoring Methodologies

The Department's Contract Manager, or designee, will monitor the Vendor's service delivery to determine if the Vendor has achieved the required level of performance for each Performance Measure identified in Section 2.10, Performance Measures and Performance Monitoring.

If the Department determines that the Vendor has failed to meet a Performance Measure, the Vendor will be contacted by the Department's Contract Manager, or designee, to address the non-compliant service delivery. The Vendor shall correct all identified non-compliant service delivery related to failure to meet the Performance Measures within 30 business days of notice.

The Department may utilize any or all of the following monitoring methodologies in monitoring the Vendor's performance under the resultant Contract, and in determining compliance with Contract terms and conditions:

(a) Desk reviews of records related to service delivery (shall include any documents and databases pertaining to the Contract and may be based on all documents and data, or a sampling of same whether random or statistical);
(b) Interviews and/or surveys with Vendor and/or Department staff; and
(c) Review of monitoring, audits, investigations, reviews, evaluations, or other actions by external agencies, as applicable (e.g., American Correctional Association, etc.).

2.12. HIPAA Business Associate Agreement

The Vendor will be required to execute a HIPAA Business Associate Agreement, included as Attachment II, and comply with all provisions of State and federal law regarding confidentiality of patient information.

2.13. Prison Rape Elimination Act (PREA)

The Vendor will comply with national standards to prevent, detect, and respond to prison rape under the Prison Rape Elimination Act (PREA), Federal Rule 28 C.F.R. Part 115. The Vendor will also comply with all Department policies and procedures that relate to PREA.

2.14. Records and Documentation

To the extent that information is utilized in the performance of the resulting Contract or generated as a result of it, and to the extent that information meets the definition of "public record," as defined in Section 119.011(12), F.S., said information is recognized by the parties to be a public record and, absent a provision of law or administrative rule or regulation requiring otherwise, shall be made available for inspection and copying by any person upon request as provided in Chapter 119, F.S. The Vendor agrees to: (a) keep and maintain public records required by the Department in order to perform the service; (b) upon request from the Department's custodian of public records, provide the Department with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law; (c) ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the Contract term and following completion of the Contract if the Vendor does not transfer the records to the Department; and (d) upon completion of the Contract, transfer, at no cost, to the Department all public records in possession of the Vendor or keep and maintain public records required by the Department to perform the service. If the Vendor transfers all public records to the Department upon completion of the Contract, the Vendor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Vendor keeps and maintains public records upon completion of the Contract, the Vendor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Department, upon request from the Department's custodian of public records, in a format that is compatible with the information technology systems of the Department. Unless a greater retention period is required by State or Federal law, all documents pertaining to the program contemplated by this RFQ shall be retained by the Vendor for a period of five (5) years after the termination of the resulting Contract or longer as may be required by any renewal or extension of the Contract. Pursuant to Section 287.058(1)(c), F.S., the Department is allowed to unilaterally cancel the Contract for refusal by the Vendor to allow public access to all documents, papers, letters, or other material made or received by the Vendor in conjunction with the Contract, unless the records are exempt from Section 24(a) of Art. I of the State Constitution and either Section 119.07(1), or Section 119.071, F.S.

The Vendor further agrees to hold the Department harmless from any claim or damage including reasonable attorney's fees and costs or from any fine or penalty imposed as a result of failure to comply with the public records law or an improper disclosure of confidential information and promises to defend the Department against the same at its expense.

2.14.1. Audit Records: The Vendor agrees to maintain records and documents (including electronic storage media) in accordance with generally accepted accounting

procedures and practices (GAAP), which sufficiently and properly reflect all revenues and expenditures of funds provided by the Department under the resultant Contract, and agrees to provide a financial and compliance audit to the Department or to the Office of the Auditor General, and to ensure that all related party transactions are disclosed to the auditor.

The Vendor agrees to include all record-keeping requirements in all subcontracts and assignments related to the resulting Contract.

2.15. Financial Specifications

2.15.1. Funding Source

This project is funded by General Revenue and is contingent upon annual appropriation by the Legislature.

2.15.2. Invoicing and Payments of Invoice

The resultant Contract will be at a fixed-rate per service. The Department will compensate the Vendor for services, as specified in Section 3.5, Price Sheet. All charges must be billed in arrears, in accordance with Section 215.422, F.S.

The awarded Vendor agrees to request compensation on a monthly basis through submission of a properly completed invoice within 30 days following the month services were rendered. Invoices must be submitted in detail sufficient for a proper pre-audit and post-audit thereof. Invoices must be accompanied by the required reports outlined in Section 2.9, General Reporting Requirements, shall be submitted to the Department's Contract Manager, or designee, and shall include all required information.

The Vendor's invoice shall include the Vendor's name, Contract number, invoice number, Federal Employer Identification Number (FEIN), unit rates, in accordance with the Price Sheet, and dates of service.

2.16. Vendor Ombudsman

A Vendor Ombudsman has been established within the Florida Department of Financial Services (DFS). The duties of this individual include acting as an advocate for Vendors who may be experiencing problems in obtaining timely payment(s) from a state agency. The Vendor Ombudsman may be contacted by calling the Department of Financial Services' at (850) 413-5516.

2.17. Modification after Contract Execution

During the term of the Contract, the Department may unilaterally require changes (altering, adding to, or deducting from the specifications) provided such changes are within the general scope of this RFQ.

The Vendor may request an equitable adjustment in the price(s) or delivery date(s), if the change affects the cost or time of performance. Such equitable adjustments require the express written approval of the Department.

The Department shall provide written notice to the Vendor 30 days in advance of any Department-required changes to the technical specifications, and/or scope of service, which affect the Vendor's ability to provide the service as specified herein. Any changes, other than purely administrative changes, will require a written change order or formal Contract amendment.

2.18. Indemnification

The awarded Vendor shall be liable, and shall indemnify, defend, and hold harmless the Department, its employees, agents, officers, heirs, and assignees from any and all claims, suits, judgments, or damages, including court costs and attorney's fees, arising out of intentional acts, negligence, or omissions by the Vendor(s), or its employees or agents, in the course of the operations of this Contract. This includes any claims or actions brought under Title 42 USC § 1993, the Civil Rights Act.

2.19. Inspector General

In accordance with Section 20.055(5), F.S., the Vendor, and any subcontractor, understands and will comply with its duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing.

2.20. Scrutinized Companies Certification

The Vendor certifies they are not listed on the Scrutinized Companies that Boycott Israel List, created pursuant to Section 215.4725, F.S., and they are not currently engaged in a boycott of Israel. If the resulting Contract exceeds $1,000,000.00 in total, not including renewal years, the Vendor certifies that they are not listed on either the Scrutinized Companies with Activities in Sudan List, or the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List created pursuant to Sections 215.473, F.S., and 215.4725, F.S., and further certifies they are not engaged in business operations in Cuba or Syria. Pursuant to Sections 287.135(5), F.S., and 287.135(3), F.S., the Vendor agrees the Department may immediately terminate the resulting Contract for cause if the Vendor is found to have submitted a false certification or if the Vendor is placed on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, the Scrutinized Companies that Boycott Israel List, or is engaged in a boycott of Israel, or has engaged in business operations in Cuba or Syria during the term of the resulting Contract. Any company that submits a bid or proposal for a Contract, or intends to enter into or renew a Contract with an agency or local governmental entity for goods or services, of any amount, must certify that the company is not participating in a boycott of Israel.

3. Contents of Quote Response

Interested cooperative purchasing Vendors on GSA Schedule 70 may submit a Quote for the provision and implementation of a turn-key Virtual Desktop Infrastructure Platform. Responses to this RFQ may be in narrative format, and shall include the following sections and information:

3.1. Introductory Letter and Executive Summary

The Vendor's quote must contain a concise explanation of the Vendor's method of delivering services in compliance with the requirements of this RFQ. This section should also contain corporate history information, the names of all officers or directors of the corporation, any information about subcontractors that the Vendor plans on using utilizing, and the identity of any director, employee, or agent who owns 5% or more of the corporation and is currently an

employee of the State of Florida. The Vendor must disclose whether any parent corporation, subsidiary, shareholder, director, employee, or other agent has ever been convicted of any crime involving fraud or deceit, and whether such Vendor is currently under investigation by any federal, state, or local law enforcement agency.

3.2. Corporate Experience and Qualifications

The Vendor must provide proof that it is registered to do business in the State of Florida. It must also give a brief corporate history, including any contractual services performed that are similar in scope to the requirements of this RFQ. The background information of the submitting Vendor, at a minimum, shall include:

- Date established;
- Ownership (public company, partnership, subsidiary, etc.);
- Primary type of business and number of years conducting primary business; and
- National accreditations, memberships in professional associations or other similar credentials.

The Vendor must list all Contracts it has been a party to that were entered into for similar services in the past five (5) years, as well as any sanctions or financial penalties that were assessed against it as part of its performance of those contracts. This should also identify any contracts that were terminated prior to original expiration date.

The Vendor is strongly encouraged to furnish references with their Quote, utilizing Attachment IV, Business Reference Form, of this RFQ. In order to qualify as current experience, services described by corporate reference shall be ongoing or shall have been completed within the 36 months preceding the issue date of this RFQ. The Department may contact these references and evaluate them using Attachment V, Reference Questionnaire, which the Department will complete.

3.3. Project Staff

The Vendor shall provide the Department with a basis for determining its understanding of the qualifications of personnel required for administrative oversight and/or management of any resulting Contract. The Vendor shall supply information related to all project staff proposed in its Quote, such as resumes or curriculum vitae, and qualifications of the following individuals to be assigned the Contract.

3.4. Service Delivery Approach

The Vendor shall provide a narrative Service Delivery Approach identifying how the Vendor will meet the Scope of Work of this RFQ, or the Vendor's quote shall be deemed non-responsive. The response should fully describe the Vendor's methodology for meeting the Department's requirements for service delivery, outlined in Section 2.0, specifically addressing each component of providing services. This section should be prepared in such a manner that it will be understandable to individuals on a programmatic and management level. Vendors should be thorough and detailed in their response. Vendors are encouraged to include any additional relevant information that would assist in evaluating the overall strength of the program.

3.5. Price Sheet

The Vendor shall provide a price sheet conforming to the format below.

3.5.1 Each Hardware component shall be itemized on a separate line with initial list price, discount, and proposed price.

3.5.2 Each Software component shall be itemized on a separate line with initial list price, discount, and proposed price.

3.5.3 Maintenance for each Hardware and Software component shall be itemized on a separate line in the Hardware and Software Maintenance table.

3.5.4 Labor necessary for consulting, project management, implementation, installation, and recurring support shall be itemized on a separate line in the Consulting Services and Recurring Support Services table, with a maximum number of hours provided per fiscal year for each proposed resource. This hourly rate should be inclusive of all fees, travel, and related expenses.

Each line item shall have an individual unit price, which shall be valid for the full term of the Contract. The Department may choose to purchase additional quantities anytime during the resultant Contract term.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

LOCATION	PC COUNT	MFN2 CIRCUIT
Apalachee CI East Unit 35 Apalachee Drive Sneads, Florida 32460 (850) 718-0688 **Apalachee CI West Unit** 52 West Unit Drive2 Sneads, Florida 32460 (850) 718-0577	164	33
Avon Park CI 8100 Highway 64 East Avon Park, Florida 33826-1100 (863) 453-3174	140	33
Baker CI 20706 US Highway 90 E Sanderson, Florida 32087-2359 (386) 719-4500	124	15
Baker CI- Work Camp 20706 US Highway 90 W. Sanderson, Florida 32087-0500 (386) 719-4500	1	2
Calhoun CI 19562 SE Institution Drive Blountstown, Florida 32424-5156 (850) 237-6500	112	15
Century CI 400 Tedder Road Century, Florida 32535-3659 (850) 256-2600	127	33
Central Florida Reception Center 7000 HC Kelley Rd Orlando, Florida 32831-2518 (407) 207-7777	256	45
Charlotte CI 33123 Oil Well Road Punta Gorda, Florida 33955-9701 (941) 833-8100	143	33
Cross City CI 568 NE 255th Street Cross City, Florida 32628 (352) 498-4741	124	33

LOCATION	PC COUNT	MFN2 CIRCUIT
Dade CI 19000 S. W. 377th Street Florida City, Florida 33034-6409 (305) 242-1900	174	33
DeSoto CI 13617 S.E. Highway 70 Arcadia, Florida 34266-7800 (863) 494-3727	150	33
Everglades CI 1599 S.W. 187th Ave. Miami, Florida 33194 (305) 228-2000	176	33
Franklin CI 1760 Highway 67 North Carrabelle, Florida 32322 (850) 697-1100	129	33
Florida State Prison 7819 N.W. 228th Street Raiford, Florida 32026-1000 (904) 368-2500	202	45
Gulf CI 500 Ike Steele Road Wewahitchka, Florida 32465-0010 (850) 639-1000 SC 790-1000	170	33
Hamilton CI 10650 SW 46th Street Jasper, Florida 32052-1360 (386) 792-5151	157	33
Hardee CI 6901 State Road 62 Bowling Green, Florida 33834-9505 (863) 767-3100	126	15
Hernando CI 16415 Spring Hill Drive Brooksville, Florida 34604-8167 (352) 754-6715	65	15
Holmes CI 3142 Thomas Drive Bonifay, Florida 32425-0190 (850) 547-8600	115	33

LOCATION	PC COUNT	MFN2 CIRCUIT
Jefferson CI 1050 Big Joe Road Monticello, Florida 32344-0430 (850) 342-0500	89	33
Lake CI 19225 U.S. Highway 27 Clermont, Florida 34715-9025 (352) 394-6146	144	21
Lancaster CI 3449 S.W. State Road 26 Trenton, Florida 32693-5641 (352) 463-4100	117	15
Lawtey CI 22298 NE County Road 200B Lawtey, Florida 32058 (904) 782-2000	87	15
Liberty CI 11064 N.W. Dempsey Barron Road Bristol, Florida 32321-9711 (850) 643-9400	137	33
Lowell CI 11120 NW Gainesville Rd Ocala, Florida 34482-1479 (352) 401-5301	213	45
Florida Women's Reception Center 3700 NW 111th Place Ocala, Florida 34482-1479 (352) 840-8000	143	33
Madison CI 382 Southwest MCI Way Madison, Florida 32340-4430 (850) 973-5300	106	33
Marion CI 3269 NW 105th Street Ocala, Florida 34475 (352) 401-6400	139	33
Martin CI 1150 S.W. Allapattah Road Indiantown, Florida 34956-4397 (772) 597-3705	126	15

LOCATION	PC COUNT	MFN2 CIRCUIT
Mayo CI 8784 US Highway 27 West Mayo, Florida 32066-3458 (386) 294-4500	125	33
New River CI P.O. Box 900 Raiford, Florida 32083 (904) 368-1500	64	15
Okaloosa CI 3189 Colonel Greg Malloy Road Crestview, Florida 32539-6708 (850) 682-0931	111	33
Okeechobee CI 3420 N.E. 168th Street Okeechobee, Florida 34972-4824 (863) 462-5400	127	33
Polk CI 10800 Evans Road Polk City, Florida 33868-6925 (863) 984-2273	159	33
Putnam CI 128 Yelvington Road East Palatka, Florida 32131-2112 (386) 326-6800	67	15
Quincy Annex 2225 Pat Thomas Parkway Quincy, Florida 32351-8645 (850) 627-5400	50	15
Reception and Medical Center P.O. Box 628 Hwy 231 Lake Butler, Florida 32054-0628 (386) 496-6000	259	45
Santa Rosa CI 5850 East Milton Rd. Milton, Florida 32583-7914 (850) 983-5800	236	45
South Florida Reception Center 14000 NW 41st Street Doral, Florida 33178-3003 (305) 592-9567	184	33

LOCATION	PC COUNT	MFN2 CIRCUIT
Sumter CI 9544 County Road 476B Bushnell, Florida 33513-0667 (352) 569-6100	138	33
Suwannee CI 5964 U.S. Highway 90 Live Oak, Florida 32060 (386) 963-6530	227	45
Taylor CI 8501 Hampton Springs Road Perry, Florida 32348-8747 (850) 838-4000	173	33
Tomoka CI 3950 Tiger Bay Road Daytona Beach, Florida 32124-1098 (386) 323-1070	125	33
Union CI 7819 N.W. 228th Street Raiford, Florida 32026-4000 (386) 431-2000	207	45
Wakulla CI 110 Melaleuca Drive Crawfordville, Florida 32327-4963 (850) 410-1895	186	33
Walton CI 691 Institution Road DeFuniak Springs, Florida 32433-1831 (850) 951-1300	97	33
Northwest Florida Reception Center 4455 Sam Mitchell Drive Chipley, Florida 32428-3501 (850) 773-6100	217	45
Zephyrhills CI 2739 Gall Boulevard Zephyrhills, Florida 33541-9701 (813) 782-5521	90	33

ATTACHMENT II
BUSINESS ASSOCIATE AGREEMENT FOR HIPAA
FDC RFQ-19-014

This Business Associate Agreement supplements and is made a part of this Agreement between the Florida Department of Corrections ("Department") and _____ ("Contractor"), (individually, a "Party" and collectively referred to as "Parties").

Whereas, the Department creates or maintains, or has authorized the Contractor to receive, create, or maintain certain Protected Health Information ("PHI,") as that term is defined in 45 C.F.R. §164.501 and that is subject to protection under the Health Insurance Portability and Accountability Act of 1996, as amended. ("HIPAA");

Whereas, the Department is a "Covered Entity" as that term is defined in the HIPAA implementing regulations, 45 C.F.R. Part 160 and Part 164, Subparts A, C, and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") and the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule");

Whereas, the Contractor may have access to Protected Health Information in fulfilling its responsibilities under its Contract with the Department;

Whereas, the Contractor is considered to be a "Business Associate" of a Covered Entity as defined in the Privacy Rule;

Whereas, pursuant to the Privacy Rule, all Business Associates of Covered Entities must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI; and

Whereas, the purpose of this Agreement is to comply with the requirements of the Privacy Rule, including, but not limited to, the Business Associate Contract requirements of 45 C.F.R. §164.504(e).

Whereas, in regard to Electronic Protected Health Information as defined in 45 C.F.R. § 160.103, the purpose of this Agreement is to comply with the requirements of the Security Rule, including, but not limited to, the Business Associate Contract requirements of 45 C.F.R. §164.314(a).

Now, therefore, in consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. **Definitions**
   Unless otherwise provided in this Agreement, any and all capitalized terms have the same meanings as set forth in the HIPAA Privacy Rule, HIPAA Security Rule or the HITECH Act. Contractor acknowledges and agrees that all Protected Health Information that is created or received by the Department and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display by the Department or its operating units to Contractor or is created or received by Contractor on the Department's behalf shall be subject to this Agreement.

2. **Confidentiality Requirements**
   A. Contractor agrees to use and disclose Protected Health Information that is disclosed to it by the Department solely for meeting its obligations under its agreements with the Department, in accordance with the terms of this agreement, the Department's established policies rules, procedures and requirements, or as required by law, rule or regulation.

B. In addition to any other uses and/or disclosures permitted or authorized by this Agreement or required by law, Contractor may use and disclose Protected Health Information as follows:

(1) if necessary for the proper management and administration of the Contractor and to carry out the legal responsibilities of the Contractor, provided that any such disclosure is required by law or that Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Contractor of any instances of which it is aware in which the confidentiality of the information has been breached;

(2) for data aggregation services, only if to be provided by Contractor for the health care operations of the Department pursuant to any and all agreements between the Parties. For purposes of this Agreement, data aggregation services means' the combining of protected health information by Contractor with the protected health information received by Contractor in its capacity as a Contractor of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

(3) Contractor may use and disclose protected health information that Contractor obtains or creates only if such disclosure is in compliance with every applicable requirement of Section 164.504(e) of the Privacy relating to Contractor Contracts. The additional requirements of Subtitle D of the HITECH Act that relate to privacy and that are made applicable to the Department as a covered entity shall also be applicable to Contractor and are incorporated herein by reference.

C. Contractor will implement appropriate safeguards to prevent use or disclosure of Protected Health Information other than as permitted in this Agreement. Further, Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Department. The Secretary of Health and Human Services and the Department shall have the right to audit Contractor's records and practices related to use and disclosure of Protected Health Information to ensure the Department's compliance with the terms of the HIPAA Privacy Rule and/or the HIPAA Security Rule.

Further, Sections 164.308 (administrative safeguards). 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies and procedures and documentation requirements) of the Security Rule shall apply to the Contractor in the same manner that such sections apply to the Department as a covered entity. The additional requirements of the HITECH Act that relate to security and that are made applicable to covered entities shall be applicable to Contractor and are hereby incorporated by reference into this BA Agreement.

D. Contractor shall report to Department any use or disclosure of Protected Health Information, which is not in compliance with the terms of this Agreement as well as any Security incident of which it becomes aware. Contractor agrees to notify the Department, and include a copy of any complaint related to use, disclosure, or requests of Protected Health Information that the Contractor receives directly and use best efforts to assist the Department in investigating and resolving such complaints. In addition, Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Protected Health Information by Contractor in violation of the requirements of this Agreement.

Such report shall notify the Department of:

1) any Use or Disclosure of protected health information (including Security Incidents) not permitted by this Agreement or in writing by the Department;

2) any Security Incident;

3) any Breach, as defined by the HITECH Act; or any other breach of a security system, or like system, as may be defined under applicable State law (Collectively a "Breach").

Contractor will without unreasonable delay, but no later than 72 hours after discovery of a Breach, send the above report to the Department.

Such report shall identify each individual whose protected health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during any Breach pursuant to 42 U.S.C.A. § 17932(b). Such report will:

1) Identify the nature of the non-permitted or prohibited access, use, or disclosure, including the nature of the Breach and the date of discovery of the Breach.

2) Identify the protected health information accessed, used or disclosed, and provide an exact copy or replication of that protected health information.

3) Identify who or what caused the Breach and who accessed, used, or received the protected health information.

4) Identify what has been or will be done to mitigate the effects of the Breach; and

5) Provide any other information, including further written reports, as the Department may request.

E. In accordance with Section 164.504(e)(1)(ii) of the Privacy Rule, each party agrees that if it knows of a pattern of activity or practice of the other party that constitutes a material breach of or violation of the other party's obligations under the BA Agreement, the non-breaching party will take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, terminate the Contract or arrangement if feasible. If termination is not feasible, the party will report the problem to the Secretary of Health and Human Services (federal government).

F. Contractor will ensure that its agents, including a subcontractor, to whom it provides Protected Health Information received from, or created by Contractor on behalf of the Department, agree to the same restrictions and conditions that, apply to Contractor, and apply reasonable and appropriate safeguards to protect such information. Contractor agrees to designate an appropriate individual (by title or name) to ensure the obligations of this agreement are met and to respond to issues and requests related to Protected Health Information. In addition, Contractor agrees to take other reasonable steps to ensure that its employees' actions or omissions do not cause Contractor to breach the terms of this Agreement.

G. Contractor shall secure all protected health information by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute and is consistent with guidance issued by the Secretary of Health and Human Services

specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, including the use of standards developed under Section 3002(b)(2)(B)(vi) of the Public Health Service Act, pursuant to the HITECH Act, 42 U.S.C.A. § 300jj-11, unless the Department agrees in writing that this requirement is infeasible with respect to particular data. These security and protection standards shall also apply to any of Contractor's agents and subcontractors.

H. Contractor agrees to make available Protected Health Information so that the Department may comply with individual rights to access in accordance with Section 164.524 of the HIPAA Privacy Rule. Contractor agrees to make Protected Health Information available for amendment and incorporate any amendments to Protected Health Information in accordance with the requirements of Section 164.526 of the HIPAA Privacy Rule. In addition, Contractor agrees to record disclosures and such other information necessary, and make such information available, for purposes of the Department providing an accounting of disclosures, as required by Section 164.528 of the HIPAA Privacy Rule.

I. The Contractor agrees, when requesting Protected Health Information to fulfill its Contractual obligations or on the Department's behalf, and when using and disclosing Protected Health Information as permitted in this Contract, that the Contractor will request, use, or disclose only the minimum necessary in order to accomplish the intended purpose.

3. **Obligations of Department**

A. The Department will make available to the Business Associate the notice of privacy practices (applicable to inmates under supervision, not to inmates) that the Department produces in accordance with 45 CFR 164.520, as well as any material changes to such notice.

B. The Department shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

C. The Department shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that impacts the business associate's use or disclosure and that the Department has agreed to in accordance with 45 CFR 164.522 and the HITECH Act.

4. **Termination**

A. Termination for Breach - The Department may terminate this Agreement if the Department determines that has breached a material term of this Agreement. Alternatively, the Department may choose to provide Contractor with notice of the existence of an alleged material breach and afford Contractor an opportunity to cure the alleged material breach. In the event Contractor fails to cure the breach to the satisfaction of the Department, the Department may immediately thereafter terminate this Agreement.

B. Automatic Termination - This Agreement will automatically terminate upon the termination or expiration of the original Contract between the Department and the Contractor.

C. Effect of Termination

(1) Termination of this agreement will result in termination of the associated Contract between the Department and the Contractor.

(2) Upon termination of this Agreement or the Contract, Contractor will return or destroy all PHI received from the Department or created or received by Contractor on behalf of the Department that Contractor still maintains and retain no copies of such PHI; provided that if such return or destruction is not feasible, Contractor will extend the protections of this Agreement to the PHI and limit further uses and disclosure to those purposes that make the return or destruction of the information infeasible.

5. **Amendment** - Both parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary to comply with the requirements of the Privacy Rule, the HIPAA Security Rule, and the HITECH Act.

6. **Interpretation** - Any ambiguity in this Agreement shall be resolved to permit the Department to comply with the HIPAA Privacy Rule and/or the HIPAA Security Rule.

7. **Indemnification** – The Contractor shall be liable for and agrees to be liable for, and shall indemnify, defend, and hold harmless the Department, its employees, agents, officers, and assigns from any and all claims, suits, judgments, or damages including court costs and attorneys' fees arising out or in connection with any non-permitted or prohibited Use or Disclosure of PHI or other breach of this Agreement, whether intentional, negligent or by omission, by Contractor, or any subcontractor of Contractor, or agent, person or entity under the control or direction of Contractor. This indemnification by Contractor includes any claims brought under Title 42 USC §1983, the Civil Rights Act.

8. **Miscellaneous** - Parties to this Agreement do not intend to create any rights in any third parties. The obligations of Contractor under this Section shall survive the expiration, termination, or cancellation of this Agreement, or any and all other contracts between the parties, and shall continue to bind Contractor, its agents, employees, contractors, successors, and assigns as set forth herein for any PHI that is not returned to the Department or destroyed.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

ATTACHMENT III
CERTIFICATION/ATTESTATION FORM
FDC RFQ-19-014

1. **Business/Corporate Experience:**
   This is to certify that the Vendor(s) has at least two (2) years of authorized business/corporate experience to conduct with the State of Florida under GSA Schedule 70, within the last five (5) years, relevant in the provision and implementation of a turn-key virtual desktop and infrastructure platform.
2. **Authority to Legally Bind the Vendor:**
   This is to certify that the person signing below is authorized to make this affidavit on behalf of the firm, its owner(s), directors and officers. This person is the person in the firm responsible for the prices and total amount of this submittal and the preparation of the response.
3. **Statement of No Involvement:**
   This is to certify that the person signing the quote has not participated, and will not participate, in any action contrary to the terms of this solicitation.
4. **Statement of No Inducement:**
   This is to certify that no attempt has been made or will be made by the Vendor to induce any other person or firm to submit or not to submit a quote with regard to this solicitation. Furthermore, this is to certify that the quote contained herein is submitted in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other non-competitive submission.
5. **Statement of Non-Disclosure:**
   This is to certify that neither the price(s) contained in this response, nor the approximate amount of this quote have been disclosed, directly or indirectly, to any other Vendor or to any competitor.
6. **Statement of Non-Collusion:**
   This is to certify that the prices and amounts in this submittal have been arrived at independently, without consultation, communications, or agreement as to any matter relating to such prices with any other Vendor or with any competitor and not for the purpose of restricting competition.
7. **Non-Discrimination Statement:**
   This is to certify that the Vendor does not discriminate in their employment practices with regard to race, creed, color, national origin, age, gender, marital status or disability.
8. **Unauthorized Alien Statement:**
   This is to certify that the Vendor does not knowingly employ unauthorized alien workers.
9. **Statement of No Investigation/Conviction:**
   This is to certify that Vendor, its affiliates, subsidiaries, officers, directors and employees are not currently under investigation by any governmental agency, and have not in the last three years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding on any public Contract.
10. **Scrutinized Companies Certification:** If value of this solicitation is greater than or equal to $1 million, then the Vendor certifies they are not listed on either the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities on the Iran Petroleum Energy Sector List, or the scrutinized companies that Boycott Israel list, or is engaged in a boycott of Israel, or has engaged in business operations in Cuba or Syria during the term of the resulting Contract.

Dated this _____ day of _____ 20__.

Name of Organization: _____

Signed by: _____

Title: _____

being duly sworn deposes and says that the information herein is true and sufficiently complete so as not to be misleading.

Subscribed and sworn before me this _____ day of _____ 20__.

Notary Public: _____

My Commission Expires: _____

ATTACHMENT IV –BUSINESS REFERENCE FORM

FDC RFQ-19-014

Vendors are required to submit with the Quote, contact information for three (3) entities it has provided with services similar to those requested in this solicitation. The Department reserves the right to contact any and all entities in the course of this solicitation evaluation in order to make a fitness determination. The Department will make only two (2) attempts to contact each entity. The Department's determination is not subject to review or challenge.

1) Name of Company/Agency: _____

Contact Person: _____

Phone Number: _____

Address: _____

Email Address: _____

2) Name of Company/Agency: _____

Contact Person: _____

Phone Number: _____

Address: _____

Email Address: _____

3) Name of Company/Agency: _____

Contact Person: _____

Phone Number: _____

Address: _____

Email Address: _____

_____
Name of Vendor

_____
Signature of Authorized Representative

_____
Date

ATTACHMENT V - REFERENCE QUESTIONNAIRE
FDC RFQ-19-014

This form will be completed by the Department utilizing the information provided on Attachment IV.

THIS BUSINESS/CORPORATE REFERENCE IS FOR: _____

NAME OF PERSON PROVIDING REFERENCE: _____

TITLE OF PERSON PROVIDING REFERENCE: _____

FIRM OR BUSINESS NAME: _____

TELEPHONE NUMBER: _____ **EMAIL ADDRESS:** _____

1. How would you describe your relationship to this business/corporate entity? (e.g. Customer, Subcontractor, Employee, Contract Manager, Friend, or Acquaintance)

_____

_____

_____

2. A. If a Customer, please specifically describe the primary type of licensed substance use disorder treatment program services, or other similar services, this entity provided to you.

_____

_____

_____

B. Generally describe the geographic area where services were provided (number of counties served, section of the state, etc.).

_____

_____

_____

C. What was the estimated population of clients served?

_____

_____

_____

3. Did this entity act as a primary provider, or as a subcontractor? If a subcontractor, to whom? Please specifically describe the type of service that was provided by the entity for which this reference is being provided.

_____

_____

4. Can you identify the number of years that this entity has provided licensed substance use disorder treatment services, or other similar services? Please provide dates to the best of your knowledge.

5. To your knowledge, did this entity perform or provide complete services, or was any portion of the services subcontracted out?

6. How many years have you done business with this business entity?

   Please Provide Dates:

7. Do you have a vested interest in this business/corporate entity? If yes, what is that interest? (i.e. employee, subcontractor, stockholder, etc.).

8. Have you experienced any problems with this business/corporate entity? If so, please state what the problem is/was and how it was resolved.

9. Would you conduct business with this business/corporate entity again? If no, please state the reason.

10. Are there any additional comments you would like to make about this business entity? Use back of form if necessary.

VERIFIED BY/DATE:

ATTACHMENT VI
VENDOR'S CONTACT INFORMATION
FDC RFQ-19-014

The Vendor shall identify the contact information for Solicitation and Contractual purposes per the requested fields of the table below.

	Vendor's Contact Person For Solicitation Purposes	Vendor's Contact Person For Contractual Purposes (should Vendor be awarded)
Name:		
Title:		
Address: (Line 1)		
Address: (Line 2)		
City, State, Zip code		
Telephone: (Office)		
Telephone: (Mobile)		
Fax:		
Email:		

_____ _____

Authorized Vendor's Signature Date

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

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

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

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

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

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

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

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

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

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

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

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

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

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

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

1.00 Definitions

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

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

2.00 Responsibilities of the Contracting Government Agency.

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

3.00 Responsibilities of the Contractor.

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

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA 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:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION

CRIMINAL JUSTICE INFORMATION SERVICES

SECURITY ADDENDUM

CERTIFICATION

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

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

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative