NEW YORK STATE | Corrections and Community Supervision

KATHY HOCHUL
Governor

DANIEL F. MARTUSCELLO III
Commissioner

Addendum #2
July 8, 2024
IFB 2024-13 – Staff Wellness Smart Mobile Application

The following are official modifications which are hereby incorporated into IFB 2024-13 – Staff Wellness Smart Mobile Application. The information contained in this addendum prevails over the original IFB language for all amendments below.

Security Terms - Appendix C

IFB #2024-13, Security Terms, have been added as follows in Appendix C.

All other terms and conditions remain the same.

_____ _____
Signature Date

_____
Print Name and Title

Applicants should monitor the following Web sites for posted updates or information:

NYS Contract Reporter: https://www.nyscr.ny.gov/ NYS DOCCS' Web site: https://doccs.ny.gov/procurement-opportunities.

APPENDIX C

Security Terms

CJIS:

At no time shall the Contractor access any criminal justice information (including criminal history record information or other sensitive criminal justice information), as defined by the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy (the "CJIS Security Policy") ***(https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view),*** contained on NYS Systems or media without complying with this Section. Any access to computer media/systems which contain criminal justice information including criminal history record information and other sensitive criminal justice information is subject to the CJIS Security Policy and its related Security Addendum (the "SA") ***(reflected and incorporated in Attachment T.2).*** The purpose of the SA is to provide adequate security for criminal justice systems and information while under the management or control of a private entity or contractor. The SA strictly limits the authorized access to criminal justice information (including criminal history record information), limits the use of the information to the specific purposes for which it is being provided, ensures the security and confidentiality of the information consistent with applicable laws and regulations, provides for sanctions, and contains such other provisions as required by the FBI Director. Upon selection, the selected Contractor and as a condition precedent for providing Services, agrees (1) to abide by the CJIS Security Policy and its related SA, and (2) to the incorporation by reference of the CJIS Security Policy and its related SA as a part of the Contract, (3) that the CJIS Security Policy and its related SA shall be incorporated by reference as a part of all subcontracts entered into by the Successful Contractor for delivery of Services, if any; and (4) that those Successful Contractor employees and subcontractor employees (Contractor Staff), if any that provide Services shall sign the form set forth as ***Attachment T.2*** hereto, referenced and incorporated in the CJIS Security Policy as the "Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification.". One copy of the signed form will be retained by the Successful Contractor and the original will be provided to the State for retention by the CJIS Information Security Officer for New York State. The State may terminate the Contract if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor, its agents and subcontractors, if any. Contractor agrees that all subcontractors, if any and agents shall be made aware of and shall agree to the terms of this section.

OFF SHORE RESTRICTIONS:

Confidential Information accessed by or provided to Contractor during the course of performing services for the State must not be stored or accessed outside of the continental United States.

COMPLIANCE WITH NYS SECURITY POLICIES AND STANDARDS:

Contractor warrants, covenants and represents that it shall comply fully with all ITS Information Security policies and procedures located at https://its.ny.gov/tables/technologypolicyindex.htm/security, this includes but is not limited to:

- Acceptable Use of Information Technology (IT) Resources Policy
- Information Security Policy
- Information Security Controls Standard
- Encryption Standard
- Vulnerability Scanning Standard
- Information Security Risk Management Standard
- Patch Management Standard
- Mobile Device Security Standard
- Mobile Device Security Standard
- Remote Access Standard
- Sanitization/Secure Disposal Standard
- Secure System Development Life Cycle (SSDLC) Standard
- Security Logging Standard

If the requirements set forth in the solicitation and/or contract are not the same as the NYS ITS policies, then the more restrictive policy applies. NYS DOCCS Directives also contain requirements for information security. Again, the most restrictive policy applies.

SEPARATION OF DUTIES

The State requires the Contractor to follow security best practices by adhering to separation of job duties, and limiting Contractor staff knowledge of Confidential Information to that which is absolutely needed to perform job duties.

ACCESS TO REGULATED DATA

New York State considers the protection of sensitive and confidential information and business systems to be of the upmost importance. The information collected and maintained by state and local government agencies is protected by a myriad of Federal and State laws and regulations. Access to and use of sensitive and confidential information is limited to authorized government employees and legally designated agents, for authorized purposes only.

To the extent that Contractor, its employees, agents or subcontractors have access to Federal, State or Local government regulated data pursuant to their responsibilities under the Contract, Contractor agrees that it will abide by the requirements of those Federal and State laws and regulations, and will require in writing its employees, agents or subcontractors to similarly abide by any such requirements including the execution of any documents or agreements required to be executed, certifying their compliance with same.

The Contractor shall maintain the security, nondisclosure and confidentiality of all information in accordance with the following clauses in performance of its activities under this Agreement. The State may terminate this Agreement if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor and any and all of its subcontractors and agents. Contractor agrees that all subcontractors and agents shall be made aware of and shall agree to the terms of this section.

Definitions:

1. "Facilities" or “facility: As used in this Section, the term "facilities" or “facility” shall mean any real property, tangible personal property, or electronic or virtual systems, or any part(s) or component(s) thereof, used to conduct State business operations, including, but not limited to, physical office or computing space, computer(s) or computer systems, telecommunications or network infrastructure (e.g., utility closet(s), conduits, hubs, switches, routers), and supporting facilities and systems (e.g., mechanical, power, cooling, security, fire protection, water), regardless of owner.

2. "Confidential Information": As used in this Section, the term “Confidential Information” shall mean all State information of which Contractor, its officers, agents, employees, and subcontractors becomes aware during the course of performing services for the State shall be deemed to be Confidential Information (oral, visual or written). Notwithstanding the foregoing, information which falls into any of the following categories shall not be considered Confidential Information:

    (a) Information that is rightfully known to the Contractor without any limitation on disclosure prior to its receipt from the State;

    (b) Information that becomes available publicly or to third parties through no act or failure on the part of the Contractor;

    (c) Information that is independently developed by the Contractor without use of Confidential Information of the State.

Contractor shall ensure that all of its agents, employees, partners or subcontractors are made fully aware of the obligations arising under the following security clauses and shall take all commercially reasonable steps to ensure their compliance with these provisions to prevent unauthorized use, access or disclosure of Confidential Information.

Failure by Contractor or its agents, employees, officers, partners or subcontractors to fully comply with the requirements of the following security clauses shall be deemed a failure to meet Contractor's obligations under this Agreement and may result in the State suspending, canceling and/or terminating the Agreement for cause and to pursue any other legal or equitable remedies available.

SECURITY PROCEDURES:

Contractor shall comply fully with all security procedures of the State clearly communicated to it in the performance of this Agreement. Contractor acknowledges that such security procedures may vary based on the specific State facility at which the Contractor is providing services. Contractor agrees that its agents, employees and subcontractors performing services on-site at State Facilities or those with logical access to State data (i.e. log-in access) shall be required to undergo the State's same security clearances as are required of the employees of the State. Specifically, before any contractor enters a DOCCS facility, each prospective and current employee of Contractor designated to work under this Agreement shall submit identifying information shall be submitted to the State and be fingerprinted. State shall arrange for the scheduling of fingerprinting, Contractor shall pay the reasonable costs not to exceed $150.00 per person of the fingerprinting. Such fingerprints shall be submitted to the Division of Criminal Justice Services for a state criminal history record check and, where authorized, to the Federal Bureau of Investigation for a national criminal history record check. DOCCS, in its sole discretion, may reject or bar from any State facility any employee or agent of the contractor or its subcontractors performing work under this contact, and such action by DOCCS shall not relieve the Contractor of the obligation to perform all work in compliance with the Contract terms. In addition, contractor must perform background checks and document results of their employees who may perform functions per this contract with DOCCS.

NONDISCLOSURE AND CONFIDENTIALITY:

Except as may be required by applicable law or a court of competent jurisdiction, the Contractor, its officers, agents, employees, partners and subcontractors shall maintain strict confidence with respect to Confidential Information to which the Contractor, its officers, agents, employees, and subcontractors have access. This representation shall survive termination of this Agreement.

The Contractor shall hold the State harmless from any loss or damage to the State resulting from the disclosure by the Contractor, its officers, agents, employees, partners and subcontractors of such Confidential Information. Agents, employees, officers, partners or subcontractors of the Contractor may be required to execute a Nondisclosure Agreement, either before or upon arrival at the work site, or if they will have access to critical State networks, equipment or data. In the event an individual may refuse to sign, Contractor will provide an alternative resource.

PRESS RELEASES:

Contractor agrees that no brochure, news/media/press release, public announcement, memorandum or other information of any kind regarding this Agreement shall be disseminated in any way to the public, nor shall any presentation be given regarding this Agreement without the prior written approval by the undersigned or the undersigned's designee from DOCCS, which written approval shall not be unreasonably withheld or delayed provided, however, that Contractor shall be authorized to provide copies of this Agreement and answer any questions relating thereto to any State or Federal regulators or, in connection with its financial activities, to financial institutions for any private or public offering or its financial advisors or auditors.

PUBLIC INFORMATION AND FOIL:

Disclosure of items related to this Agreement shall be permitted consistent with the laws of the State of New York and specifically the Freedom of Information Law (FOIL) contained in Section 87 of the Public Officers Law. Consistent with FOIL and applicable laws: The State shall take reasonable steps to protect from public disclosure any of the records relating to this procurement that are otherwise exempt from disclosure under FOIL; information constituting trade secrets or critical infrastructure information, for purposes of FOIL, must be clearly marked and identified as such upon submission; if the Contractor intends to seek an exemption from disclosure of these materials under FOIL, the Contractor shall, at the time of submission, request the exemption in writing and provide an explanation of why the disclosure of the identified information would cause substantial injury to the competitive position of the Contractor; or (ii) why the information constitutes critical infrastructure information which should be exempted from disclosure pursuant to §87(2) of FOIL. Acceptance of the identified information by the State does not constitute a determination that the information is exempt from disclosure under FOIL; and determinations as to the availability of the identified information will be made in accordance with FOIL at the time a request for such information is received by the State.

FEDERAL OR STATE REQUIREMENTS:

In the event that it becomes necessary for Contractor to receive Confidential Information which Federal or State statute or regulation prohibits from disclosure, Contractor hereby agrees to return or destroy all such Confidential Information that has been received from the State when the purpose that necessitated its receipt by Contractor has been completed. In addition, Contractor agrees not to retain any Confidential Information which Federal or State statute or regulation prohibits from disclosure after termination of the Agreement. Notwithstanding the foregoing, if the return or destruction of the Confidential Information is not feasible, Contractor agrees to extend the protections of the Agreement for as long as necessary to protect the Confidential Information and to limit any further use or disclosure of that Confidential Information. If Contractor elects to destroy Confidential Information, it shall use reasonable efforts to achieve the same and notify the State accordingly. Contractor agrees that it will use all appropriate safeguards to prevent any unauthorized use or unauthorized disclosure of Confidential Information which Federal or State statute or regulation prohibits from disclosure. Contractor agrees that it shall immediately report to the State the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information. Contractor shall also report the discovery of any unauthorized use or unauthorized disclosure of such Confidential Information of any New York State agency information directly to that New York State agency. The State may terminate this Agreement if it determines that Contractor has violated a material term of this section. The terms of this section shall apply equally to Contractor and any and all of its subcontractors and agents. Contractor agrees that all subcontractors and agents shall be made aware of and shall agree to the terms of this section.

DATA OWNERSHIP, MIGRATION, ACCESSIBILITY, LOCATION, STORAGE, TRANSPORT, PROTECTION AND DESTRUCTION

- Data Ownership: All State data is owned exclusively by the State and will remain the property of the State. Contractor is permitted to use data solely for the purposes set forth in the solicitation and the Contract, and for no other purpose. At no time shall the Contractor access, use, or disclose any confidential information (including but not limited to personal, financial, health, or criminal history record information or other sensitive criminal justice information) for any other purpose. The Contractor is strictly prohibited from releasing or using data or information for any purposes other than those purposes specifically authorized by the State. Contractor agrees that State data shall not be distributed, used, repurposed, transmitted, exchanged or shared across other applications, environments, or business units of the contractor or otherwise passed to other contractors, agents, subcontractors or any other interested parties, except as expressly and specifically agreed to in writing by the State. Contractor shall be strictly

prohibited from using State Data in any fashion other than that defined herein or authorized in writing by the State.

- Data Storage, Access and Location: The Contractor must ensure that all State Data related to this Contract is stored within CONUS, in a controlled access environment to ensure data security and integrity. All access to State Data, physical or virtual, must be conducted within CONUS and have adequate security systems in place to protect against the unauthorized access to the facilities and data stored therein. The Contractor shall not send or permit to be sent to any location outside of the CONUS, any State data related to this Contract. Contractor will provide the State a list of the physical locations where the Data is stored at any given time and will update that list if the physical location changes. Access into and within the facilities must be restricted through an access control system that requires positive identification as well as maintains a log of all accesses (e.g., date and time of the event, type of event, user identity, component of the information system, outcome of the event). The Contractor shall have a formal procedure in place for granting computer system access to the data and to track access. Access for projects outside of those approved by the State are prohibited.

- Physical Data Transport: The Contractor shall use, if applicable, reputable means to physically transport State data. Deliveries must be made either via hand delivery by an employee of the Contractor or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor's offices, to and from subcontractors, and to the State.

- Data Protection and Transmission: Contractor shall use appropriate means to preserve and protect State data. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. All State Data in transit and at rest will be encrypted. At a minimum, cryptographic modules used for Data transmission must be validated to FIPS 140-2 for the protection of sensitive information (http://csrc.nist.gov/groups/STM/cmvp/index.html).

- Data Return and Destruction: At the expiration or termination of the Contract, the Contractor must provide the State with a copy of the State data, including metadata and attachments, and give the State continued access to State data for no less than ninety (90) days beyond the expiration or termination of the Contract. Contractor will provide the State with the same post-termination data retrieval assistance that Contractor generally makes available to all customers. Thereafter, Contractor shall destroy State data from its systems and wipe all its data storage devices to eliminate any and all State data from Contractor's systems The sanitization process must be in compliance NYS Security Policy NYS-S13-003, https://www.its.ny.gov/document/sanitizationsecure-disposal-standard and, where required, CJIS sanitization and disposal standards. If immediate purging of all data storage components is not possible, the Contractor will certify that any data remaining in any storage component will be safeguarded to prevent unauthorized disclosures. Contractor must then certify to the State, in writing, that it has complied with the provisions of this paragraph. The State may withhold payment to Contractor if State data is not released to the State in accordance with the preceding sections.

- Contractor must, in accordance with applicable law and the instructions of the State, exercise due care for the protection of data, and maintain appropriate data integrity safeguards against the deletion or alteration of such data. In the event that any data is lost or destroyed because of any act or omission of the Contractor or any non-compliance with the obligations of this Contract, then Contractor shall, at its own expense, use its best efforts in accordance with industry standards to reconstruct such data as soon as feasible. In such event, Contractor shall reimburse the State for any costs incurred by the State in correcting, recreating, restoring or reprocessing such data or in providing assistance therewith.

- Contractor agrees that any and all State data will be stored, processed and maintained solely on designated target devices, and that no State data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that device or storage medium is a

necessary and approved component of the authorized business processes covered in the Contract and or any addendum thereof, or the Contractor's designated backup and recovery processes, and is encrypted in accordance with all current Federal and State statutes, regulations and requirements.

INFORMATION SECURITY BREACH AND NOTIFICATION ACT

In accordance with the Information and Security Breach Notification Act (ISBNA) (Chapter 442 of the Laws of 2005, as amended by Chapter 491 of the Laws of 2005), a Contractor with the State shall be responsible for all applicable provisions of the ISBNA and the following terms herein with respect to any "private information" (as defined in the ISBNA) received by or on behalf of ITS under this Contract.

- Contractor shall supply the State with a copy of its notification policy, which shall be modified to be in compliance with this provision.
- Contractor must encrypt any database fields and backup tapes in their systems that contain private information, as set forth in the ISBNA.
- Contractor must ensure that private information is encrypted in transit to/from their systems.
- In general, contractor must ensure that private information is not displayed to users on computer screens or in printed reports; however, specific users who are authorized to view the private data elements and who have been properly authenticated may view/receive such data.
- Contractor must monitor for breaches of security to any of its systems that store or process private information owned by the State.
- Contractor shall take all steps as set forth in ISBNA to ensure private information shall not be released without authorization from DOCCS.

DATA BREACH - REQUIRED CONTRACTOR ACTIONS

Data/ Confidential Information Breach is defined by the ISBNA and any Data/ Confidential Information accessed purposefully or accidentally without proper authorization by DOCCS.
Unless otherwise prohibited by law, in the event of a Data/ Confidential Information Breach, the Contractor shall:

- In the event of a confirmed breach of DOCCS Data/ Confidential Information, Contractor shall provide DOCCS initial notification within four (4) hours of a confirmed incident and commence an investigation in cooperation with DOCCS to determine the scope of the breach. Detailed, follow up notifications will be provided to DOCCS by Contractor within forty-eight (48) hours of the initial confirmed incident.
- Contractor shall also take immediate and necessary steps needed to restore the information security system to prevent further breaches.
- Contractor is to first seek consultation and receive authorization from DOCCS prior to notifying the individuals whose personal identity information was compromised by the breach of security. Contractor will coordinate all communication regarding the Data Breach with DOCCS and Authorized User(s).
- Contractor shall be responsible for providing all notices required by the ISBNA and for all costs associated with providing said notices, if contractor is determined to be at fault based on results of an investigation.
- Contractor shall cooperate with DOCCS in attempting to prevent the future recurrence of such security breaches.
- Contractor shall place corrective action in the timeframe required by DOCCS. If Contractor is unable complete the corrective action within the required timeframe, in addition to any other remedies available, DOCCS may contract with a third party to provide the required services until corrective actions and services resume in a manner acceptable to DOCCS, or until DOCCS has completed a new procurement for a replacement service system. The Contractor will be responsible for the cost of these services during this period.
- If contractor is determined to be at fault based on results of an investigation, the State reserves the right to require commercially standard credit monitoring for any and all individuals affected by the data breach at the sole expense of the Contractor for a period not to exceed 12 months, which shall begin 30 days following the notice of offer from the Contractor of such credit monitoring to those affected individuals,

which shall be within a reasonable time following the identification of such affected individuals. DOCCS reserves the right to require notice by regular or electronic mail.

Nothing herein shall in any way (a) impair the authority of the OAG to bring an action against Contractor to enforce the provisions of the New York State Information Security Breach Notification Act (ISBNA) or (b) limit Contractor's liability for any violations of the ISBNA or any other applicable statutes, rules or regulations.

Provider Removal: If a Contractor becomes aware that any Provider it has contracted with to work for DOCCS becomes a potential unacceptable risk to the State, the Contractor shall immediately notify DOCCS and jointly decide if it is necessary to remove that Provider from the site. If a Provider is removed, the Contractor will propose a qualified substitute. DOCCS may waive the removal of a Provider by providing a written waiver to the Contractor. Should DOCCS find a Provider to be an unacceptable risk to the State, DOCCS shall notify the Contractor and may request that the Contractor provide a replacement.

Contractor will maintain a Master File (electronic) for each Provider servicing DOCCS per this contract. The Master File must include: qualifications, certifications, licenses, and background checks.

Attachment T.2

FBI CJIS Security Addendum and Certification

Contractor is permitted to use Criminal Justice Information (CJI) solely for the purposes of performing the services as described in the Contract, and for no other purpose. At no time shall the Contractor access any criminal justice information (including criminal history record information or other sensitive criminal justice information) as defined by CJIS Security Policy, contained on the State's or Authorized Users Systems or media without complying with this Addendum. Any access to computer media/systems which contain criminal justice information including criminal history record information and other sensitive criminal justice information is subject to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy, specifically the Security Addendum (SA). (http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center).

The purpose of the SA is to provide adequate security for criminal justice systems and information while under the management or control of a private entity or contractor. The SA strictly limits the authorized access to criminal justice information (including criminal history record information), limits the use of the information to the specific purposes for which it is being provided, ensures the security and confidentiality of the information consistent with applicable laws and regulations, provides for sanctions, and contains such other provisions as required by the FBI Director. The Contractor as a condition precedent for providing Contract services for the benefit of the State and DOCCS agrees:

(1) to abide by the SA, and (2) to the incorporation by reference of the SA as a part of the Contract, (3) that the SA shall be incorporated by reference as a part of all subcontract entered into by the Contractor the purpose of which is of the delivery of Contract Services, if any; and (4) that those Contractor employees and subcontractor employees (Contractor Staff), if any that provide Contract Services shall sign the form entitled, "Federal Bureau of Investigation Criminal Justice Information Services Security Addendum Certification" as set forth below.

One copy of the signed form will be retained by the Contractor and the original will be provided to DOCCS for retention by the CJIS Information Security Officer for New York State.

The State may terminate the Contract if it determines that Contractor has violated a material term of this Section. The terms of this section shall apply equally to Contractor, its agents and subcontractors, if any. Contractor agrees that all subcontractors, if any and agents shall be made aware of and shall agree to the terms of this section.

CJIS SA Certification

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM CERTIFICATION

I hereby certify that I have read and am familiar with the contents of (1) the Security Addendum; (2) the CJIS Security Policy.

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

_____ _____

Signature of Contractor Employee Date

Print Name: _____

_____ _____

Signature of Contractor Representative Date

Print Name: _____