SOLICITATION 9594CS26Q0016
ATTACHMENT J-1: SECTION C — STATEMENT OF WORK (SOW)
Location Tracking Services Utilizing Global Positioning System (GPS) and Related Technologies
Court Services and Offender Supervision Agency (CSOSA)

C.1 Purpose

The Court Services and Offender Supervision Agency (CSOSA) require a comprehensive, secure, and reliable solution to support the location tracking of offenders under community supervision. The Contractor shall provide all GPS equipment, monitoring services, data management, system access, training, expert testimony, technical support, and transition services necessary to meet CSOSA's operational requirements.

C.2 Background

CSOSA supervises offenders on probation, parole, or supervised release within the District of Columbia. Since 2008, electronic location monitoring has been used to enforce curfews, monitor movement, and respond to violations. GPS technology allows high-risk offenders to be supervised in the community while maintaining public safety.

CSOSA anticipates an average of **300 active GPS-monitored offenders per day** for this requirement. Actual daily usage may fluctuate and may be higher or lower depending on operational demands.

C.2.1 CSOSA has relied upon electronic monitoring to conduct location tracking of offenders since 2008 when it began using Global Positioning System (GPS) tracking of high-risk offenders. CSOSA plans to continue the use of location monitoring in a risk-based model supervision.

C.2.2 CSOSA uses location tracking for the highest-risk offenders. Location tracking is used to enforce curfews, establish prohibited/restricted zones and assess and monitor offender movement in the community. Location tracking is a tool that allows CSOSA to provide heightened supervision of high-risk offenders while allowing such offenders to productively rehabilitate in the community.

C.3 Scope of Services

C.3.1 CSOSA requires location tracking services that utilize location tracking equipment, which incorporate multiple technologies such as GPS, Wi-Fi sniffing, cellular, and radio frequency (RF) technology, client management system (CMS) and mobile applications, data analysis, standard and customized reports, customer support, training, monitoring center service center twenty-four hours per day, seven days per week, and expert testimony in court proceedings as required by the Government.

C.3.2 The Contractor shall provide all equipment, equipment maintenance, equipment upgrades, software maintenance and updates, and user training for the system. The Contractor shall provide equipment upgrades or software updates in order to ensure CSOSA is using the most recent generation of location tracking equipment and technology throughout the life of the purchase order.

C.3.3 The Contractor agrees to only invoice CSOSA for units that are actively in use. The Contractor shall not invoice for units maintained on-the-shelf and it shall not invoice for units that have been deactivated from active tracking. CSOSA will make efforts to recover lost units. CSOSA shall not be responsible for the replacement cost for any damaged, lost, stolen, or unrecoverable units.

C.3.4 The Contractor shall replace units due to failures or deficiencies that prevent the units from monitoring the offenders' movements and locations.

C.3.5 The maximum average number of tracking devices/offenders actively monitored per day during the base period and each option period is 300. The devices in use may fluctuate daily.

C.4 Equipment Requirements

C.4.1 Include multiple technologies such as GPS, cellular/mobile telephone networks, WiFi sniffing, or RF beacons to gather, store, and transmit offender location data.

C.4.2 Utilize multiple cellular networks, network towers, and their respective roaming partners to ensure access throughout the United States for communications to and from the unit.

C.4.3 Easily pair with an accessory RF beacon as needed, at the sole discretion of the Contracting Officer’s Representative (COR), to confirm the offender’s presence at a designated location, or where the RF beacon is placed.

C.4.4 Deactivated devices may be reactivated on-line via the Client Management System (CMS) by CSOSA personnel if the device has been recharged.

C.5 Reliability and Tamper Detection

C.5.1 The Contractor shall provide units that:

1. Have tamper-resistant straps that vary in size, adjust to fit, and do not pose a safety hazard or unduly restrict activities of the offender.

2. Render clips, snaps, pins, and connectors unusable if the device/strap is removed.

3. Issue tamper alerts differentiated by type (at a minimum, strap tampering, communication interference, shielding, and jamming).

4. Will function reliably under normal atmospheric and environmental conditions.

5. Map representations of GPS latitude and longitude data accurately within a tolerance of 16 feet (4.9 meters).

C.6 Battery Requirements

C.6.1 Provide battery charge life of at least 48 hours in optimal conditions.

C.6.2 A low battery warning (such as a vibration or audible notification). The unit shall repeat this warning at fixed time intervals until the battery charge expires or until the unit is placed on a charger.

C.6.3 Confirm that a device is no longer communicating location data because of an offender failing to charge the device after receiving a series of low-battery alerts.

C.7 Communication & Data

C.7.1 Are capable of one or more methods of instant communication with the offender (e.g., audible alerts, voice communication and/or vibration).

C.7.2 Allow CSOSA staff to initiate instant communication with the unit and change alert settings.

C.7.3 Are FCC-certified.

C.7.4 In the absence of a GPS signal, record cell tower information or Wi-Fi location.

C.7.5 Distinguish among types of tracking employed by the device, such as GPS, Wi-Fi, or cellular location tracking for each location point and make this data available to end users.

C.7.6 Provide a GPS track point collection rate of at least one point every one minute and transmit GPS track points to the CMS at least one time approximately every 10 minutes under normal environmental and atmospheric conditions.

C.7.7 If the device goes into sleep mode when the offender is at rest, any location coordinates from the moment the offender resumes movement will be available to record the movement.

C.7.8 Provide a “pursuit mode” in which the device responds to commands manually toggled by CSOSA staff to increase or decrease the GPS track point collection and transmission interval.

C.7.9 Identify immediately breaches of exclusion and inclusion zones.

C.7.10 Store data should the unit lose communication with the network. No loss of any un-transmitted data should occur if the battery is depleted or contact with the network is unavailable.

C.7.11 Upon reconnecting to the network, transmit all stored data.

C.7.12 Store a minimum of ninety inclusion/exclusion zones and schedules in the onboard memory.

C.7.13 Encrypt all data transmitted to and from the device to prevent interference and duplication.

C.8 Contractor Services

C.8.1 Client Management System (CMS)

C.8.1.1 The Contractor shall provide a web-based CMS, accessible 24 hours per day, 7 days per week, and 365 days per year.

C.8.1.2 The CMS shall be accessed over a secure link via SSL on HTTPS with 256-bit encryption via a username and password or other secure login method.

C.8.1.3 The CMS shall provide end users the capability to view location data on a map to identify the location of GPS coordinates or other means of location tracking.

C.8.1.4 The mapping software used shall have zoom and panning capabilities as well as the ability to identify approximate street addresses.

C.8.1.5 Mapping should include standard, satellite, and street view capabilities in the Washington, DC Metropolitan Area.

C.8.1.6 The CMS shall allow the user to configure alerts for when an offender has entered an exclusion zone.

C.8.1.7 The supervision officer shall be able to toggle the alert of exclusion zone entry audible or nonaudible for the offender and for the supervision officer.

C.8.1.8 The CMS shall also notify the Community Supervision Officer (CSO) as the event occurs, notating within the CMS the actual time the offender enters and/or exits a geographical area of

exclusion or engages in activity that triggers an alert.

C.8.1.9 The CMS shall provide accessible data containing a listing of the names and unique identifiers of all offenders actively and historically monitored by the Contractor's equipment, associated transmitter/receiver serial numbers, current real-time status of each offender referencing the most recent event that was reported for each offender.

C.8.1.10 There shall also be access to inactive/archived offender information.

C.8.1.11 The CMS shall allow CSOSA the capability to create custom notification profiles by CSO and by offender alerting CSOSA to violation events.

C.8.1.13 Notification profiles shall include the CSO(s) to be contacted (including simultaneous multiple-party notification) and methods of contact (phone, email, text, etc.).

C.8.1.14 The Contractor shall provide CSOSA users with real-time remote web-based access to its monitoring system to view, print, download, and enter/modify offender monitoring information, and to access:

a. Offender tracking information and location
b. Device events and alerts
c. Battery life
d. Schedules
e. Multiple CSOSA offenders (Grouped by CSOSA organizational units, i.e., division, branch, or team).
f. Enrollment
g. Data analytics
h. Reports

C.8.1.15 Users shall have ability to run reports by officer caseload and any CSOSA organizational unit (team, branch, division, or agency) and by access level (CSO, SCSO, BCs, DADs, OD's Office).

C.8.1.16 The CMS shall store an unlimited number of pre-defined zones which can be applied to all offenders and which do not generate immediate alerts to CSOSA.

C.8.1.17 Users shall be able to activate zone in batch and individually.

C.8.1.18 The CMS shall provide capabilities, such as:

a. Statistical tools to help CSOs quickly identify and prioritize highest risk offenders.
b. Easy to view dashboard and reports that offer insights into:
    i. Travel patterns.
    ii. Numbers of alerts.
    iii. Proximity to risk locations.

iv. Frequency and duration of appearances at “known” locations or “unknown” locations.
v. Last known locations within a minute, hour, day, etc. of key events (like a stop in transmission, an alert, etc.).
vi. Day-by-day, hour-by-hour perspective of an offender’s activities (i.e. establishing a normal pattern of life).

C.8.1.14 The CMS shall have standard reports that allow for the interpretation of technical information, and the ability to generate and return data in PDF, Microsoft Excel and other common data formats.

C.8.1.15 The CMS shall be capable of providing daily violation reports of all violation notifications from the previous twenty-four hours.

C.8.1.16 The Contractor shall possess the ability to develop and generate new reports as requested by CSOSA, and in a format approved by the COR.

C.8.1.17 The Contractor shall complete all requests for customized and new reports within seven calendar days of the COR’s request, unless otherwise agreed to by the COR.

C.8.1.18 The Contractor shall provide strap false tamper statistics.

C.8.1.19 The Contractor shall provide the COR with a monthly lost equipment report. The lost equipment report shall be provided no later than the tenth day of the month for equipment lost during the previous month.

C.8.1.20 The Contractor shall provide a crime scene correlation capability. Crime scene correlation capability shall include the ability to provide tracking locations for all offenders on location monitoring in relation to a crime or location-of-interest within a specified timeframe.

C.8.1.21 Users shall be able to draw on a map or identify by address a location-of-interest and by user-specified timeframes to determine if any location-tracked offenders were present and to trace the movements of those offenders.

C.8.1.22 Users shall be able to perform “live” point tracking, in which the user draws on a map or identify by address a location-of-interest and sees any location-tracked offenders present and to their movements of those offenders.

C.8.1.23 The Contractor shall provide GPS Data/Subpoena Request reports quarterly to the COR and/or designated CSOSA Representative.

C.8.2 Mobile Applications

C.8.2.1 The Contractor shall provide a mobile software application for users which utilizes an authorized username and login to access and manage system features and data stored in the CMS.

C.8.2.2 The Contractor shall provide a mobile software application for offenders that provides for remote check-in, offender identity verification, violation alerts, and messaging or other forms of communication between the officer and offender.

C.8.2.3 The application may provide non-location-based communication or supervision features

for low-risk offenders.

C.8.2.4 The mobile software application for offenders may be integrated with, or issued independently of, an offender-worn tracking device.

C.8.2.5 Any mobile software application(s) shall be functional with iOS and Android operating systems.

C.8.3 Monitoring Center

C.8.3.1 The Contractor shall provide a monitoring center to support the operations of this purchase order.

C.8.3.2 The monitoring center shall be appropriately staffed and operate twenty-four hours per day, seven days per week, including holidays. This includes all systems, hardware and software, communications, and building support services.

C.8.3.3 The Contractor shall provide an in-house secure confidential monitoring center and help-desk facility with an uninterruptible power source, firewall protections, and a backup disaster recovery plan.

C.8.3.4 The Contractor shall provide a copy of the backup disaster recovery plan to the COR at the Post Award meeting, and whenever it is updated but no less than annually, no later than 30 days after the start date of each option period of performance.

C.8.3.5 The monitoring center shall be capable of providing notification to multiple persons/agencies via text message, e-mail, and voice communication. Communication may occur with offenders, CSOSA staff, or other parties as directed by the COR.

C.8.3.6 The monitoring center shall provide live agent monitoring services who execute steps to notify CSOSA staff and/or offenders of certain events or violations generated by the device in accordance with the Monitored Events Protocol. The CSOSA Monitored Events Protocol is attached (see Appendix J-x).

C.8.3.7 CSOSA reserves the right to modify the Monitored Events Protocol procedures after the commencement of this task order. The COR will notify the Contractor in writing of any modification to the Monitored Events Protocol.

C.8.3.8 The monitoring center shall record all phone calls or any message transmitted by a live staff person in the monitoring center.

C.8.3.9 The Contractor shall provide audio files of recorded communication to the COR upon request.

C.8.3.10 The monitoring center shall generate an event report documenting each step taken for each location tracking event.

C.8.3.11 The Contractor shall store this report in the CMS and make it retrievable to end users.

C.8.3.12 The monitoring center facility, equipment, data transmissions, and data storage shall be secure.

C.8.3.13 The Contractor’s facility shall be alarmed and monitored by a local law enforcement

agency or security company.

C.8.3.14 The alarm line shall be a tamperproof dedicated circuit and shall not be exposed to any person or thing that could alter or damage the line.

C.8.3.15 The monitoring center shall be equipped with automated fire detection and suppression equipment.

C.8.3.16 The monitoring center shall have a backup power supply to maintain continuous operations in the event of failures of normal utility power.

C.8.3.17 The monitoring center shall have duplicate computers with the ability to, at a minimum, permit restoration of data collection and user monitoring/solution services within thirty minutes after computer failure.

C.8.3.18 The monitoring center shall have duplicate data storage devices and automatic re-establishment of the duplicate databases upon replacement of the failed storage device.

C.8.3.19 Security of the Monitoring Center.

a. The Contractor shall provide the computer hardware necessary for the operation and twenty-four hours per day, seven days per week, continuous tracking and monitoring of offenders assigned to location monitoring tracking devices.

b. The Contractor shall provide secure transmission and storage of data relating to the crime scene correlation of location monitoring data and local law enforcement crime/incident reports.

c. The Contractor's computer system shall be ventilated and equipped with a hot redundancy system with, at a minimum, dual controllers.

d. The Contractor shall ensure that all data, data transmissions and data storage are kept confidential.

e. Within three days of this task order award, the Contractor shall provide a copy of its security policies and procedures for its network security, application security, data transmission security, data storage security, and physical security.

C.8.3.20 The Contractor shall provide multilingual services, at a minimum including Spanish, and other languages as requested by COR.

C.8.4 Customer Support

The Contractor shall, at a minimum, perform the following:

C.8.4.1 Provide a staffed communication system utilizing at minimum a toll-free telephone number and email access, available twenty-four hours per day, seven days per week.

C.8.4.2 Configure location tracking devices individually or in batch with conditions of supervision, including modified conditions and deleted conditions, within thirty minutes of the request from the COR or an authorized designee.

C.8.4.3 Immediately activate or deactivate a location tracking device on request from the COR or an authorized designee.

C.8.4.4 Provide immediate notification via telephone, text message, and email during business and non-business hours to the authorized designee or the COR when an offender incurs a violation event.

C.8.4.5 Receive verifiable confirmation via a telephone call from the monitoring center to the designated contact(s) to confirm that all immediate violation notifications were received by the supervising agent.

C.8.4.6 The Contractor shall be responsible to maintain any call trees to be utilized when contacting designated personnel to report alerts.

C.8.4.7 The Contractor shall be responsive to any requests via email or telephone from the COR or an authorized designee within thirty minutes of the request.

C.8.4.8 Notify the COR within thirty minutes by telephone and email when any services provided within this purchase order have been, or will be, interrupted for any length of time and for any reason.

C.8.5 Inventory Management

C.8.5.1 The Contractor shall maintain no fewer than 100 devices, excluding lost devices, for immediate activation. When the inventory falls below 100 units, the Contractor shall ship 50 replacement units by overnight delivery at the cost of the Contractor.

C.8.5.2 The Contractor shall provide CSOSA with the most recent version of GPS tracking devices available at the task order's fixed unit price.

C.8.5.3 The COR has sole discretion to determine the number of consumables and the number of total location monitoring units activated during the duration of this task order.

C.8.5.4 The Contractor shall supply sufficient nondurable items (i.e., spare straps, chargers and all other necessary parts for attaching and maintaining equipment/units) to allow timely installation and the servicing of current inventory.

C.8.5.5 Return shipping to the Contractor of excess or non-operational equipment shall be conducted by the COR in accordance with the shipping method required by the Contractor. All shipping expenses are the responsibility of the Contractor.

C.8.5.6 The Contractor shall maintain equipment and spares in good operating condition and arrange for prompt repair or replacement. The device shall be bench tested and certified as new for operation. The Contractor is responsible for all repair, replacement, and shipping costs.

C.8.5.7 The Contractor shall provide installation kits containing all necessary equipment and instructions to install, activate, deactivate, remove, and clean the device

C.8.6 API Integration

C.8.6.1 Application Programming Interface (API). The Contractor shall provide a Representational State Transfer (REST) Application Programming Interface (API) affording CSOSA the opportunity to fetch records relevant to its use of the Contractor's Case Management System (CMS) on demand over a secured Hypertext Transport Protocol (HTTPS) connection. The API shall:

C.8.6.2 Make changes (i.e., insert/update/delete operations) performed against the Contractor's CMS accessible within five minutes.

C.8.6.2 Be accessible to authorized CSOSA staff within thirty days of purchase order award.
C.8.6.2 Accept JavaScript Object Notation (JSON) blocks as requests.
C.8.6.2 Return JSON blocks as responses.
C.8.6.3 Include endpoints for retrieving each of the following categories of records:

a. System user records identifying and characterizing CSOSA and vendor agents (e.g., monitoring center staff) who have inserted/updated/deleted records related to CSOSA offenders.
b. Offender records identifying and characterizing CSOSA offenders who are subject to monitoring during the task order period.
c. Device records identifying and characterizing the physical hardware (including transmitters and RF beacons) provided to CSOSA under the task order.
d. Device status records characterizing the state (e.g,, in inventory, active, lost, needs recovery, non-functional/damaged, returned to vendor) of each device provided to CSOSA under the task order.
e. Activation periods identifying the date and time at which an identified device was attached to, in the case of a transmitter, or assigned to, in the case of an RF beacon, an identified offender by an identified CSOSA agent.
f. Alert records characterizing non-location events (e.g., zone violations, tampering/shielding/jamming detections, low-battery, dead battery) emitted by a device during an activation period.
g. User notes and/or status records associated with the alert.
h. Tracking records reflecting location (expressed as latitude and longitude coordinates in a specified projection such as WGS 84) of a specific device at a specific time.
i. Invoice periods, line items, unit costs, and billable unit counts sufficient to support invoices and CSOSA audits.
j. The automated data feed (data exchange) must be bi-directional.

C.8.7 Expert Testimony

C.8.7.1 The Contractor shall be competent to attest to its methodology and performance in any legal proceedings if called upon or subpoenaed to testify on behalf of CSOSA.

C.8.7.2 If required to provide testimony, the Contractor shall provide a subject matter expert (SME) to support location monitoring tracking and other data reported by the location monitoring device.

C.8.7.3 The SME shall possess experience in the location monitoring offender tracking industry, a degree in a related field, and prior experience providing expert testimony on the subject of offender location monitoring. CSOSA reserves the right to

request additional information to verify the required experience and qualifications.

C.8.7.4 The Contractor's SME shall be available on forty-eight hours notice and provide certified copies of any documentation requested by the Government or otherwise needed to support testimony.

C.8.7.5 The Contractor's SME shall be available on forty-eight hours notice and provide certified copies of any documentation requested by the Government or otherwise needed to support testimony.

C.8.7.6 The Contractor shall notify the COR immediately upon receipt of any legal process requiring disclosure of offender records.

C.8.7.7 The Contractor shall not release any information without authorization from CSOSA.

C.8.8 Training

C.8.8.1 The Contractor shall provide at least two initial training sessions in-person or via teleconference for up to 30 CSOSA personnel from CSOSA's GPS and Rapid Engagement Teams (split into two groups of 15) concerning the operation and installation of the equipment and systems specified under this task order within fourteen calendar days following the post-award meeting. Any in-person training sessions shall take place at a location determined by CSOSA within the Washington, DC, Metropolitan Area.

C.8.8.2 The training shall include verbal, written, and hands-on instructions and demonstrations concerning use of the software system and hardware/equipment.

C.8.8.3 The following training shall be available in both web-based or live in-person formats:

a. The Contractor shall provide training to all CSOSA users of the CMS and related remote applications (up to 400 personnel). These training modules shall be provided by the Contractor in-person or via a live web-based venue that permits one hundred participants at any one time. The forum used for training shall allow for participants to ask and have questions answered during the training. The forum used for training shall accommodate a member of CSOSA's program office to co-facilitate the training with privileges to read, answer, and remove posts by participants.

b. The Contractor shall also make available self-paced, web-based training modules on the CMS and related remote applications.

c. The Contractor shall also make available self-paced, web-based training modules on the CMS and related remote applications.

d. As necessary, the Contractor shall provide additional in-person or web-based training to update all CSOSA users on changes to the Contractor's software system or hardware/equipment.

e. All training provided by the Contractor under this task order (other than the answering of routine questions received over the course of performance) shall be coordinated with and approved by the COR.

C.8.8.4 The Contractor shall provide a proposed training schedule at the post-award meeting. The Contractor's proposed training schedule shall be designed to complete this training within sixty calendar days of the post-award meeting.

C.8.8.5 Train CSOSA personnel to provide the information provided by the contractor in Section C.8.8.

C.8.9 Data Ownership & Transition

C.8.9.1 The Contractor shall maintain all offender records associated with the task order for the task order life and be subject to inspection and examination by authorized CSOSA personnel.

C.8.9.2 The Contractor shall return to CSOSA all offender records and back-up copies in a usable format (example txt, csv) of the records within sixty days after the purchase order expiration.

C.8.9.3 Transition Plans. Within seven days of award, the Contractor shall develop and submit a transition plan that identifies the activities necessary to meet all aspects of this requirement. The Contractor shall clearly demonstrate the ability to prevent any break in service either transitioning into or away from the purchase order.

C.8.9.4 Transition In. The transition plan shall clearly demonstrate the ability to manage the seamless transfer and transition of this task order. The proposed implementation plan shall include, but not be limited to:

a. Seamless plan for initial mass device installation
b. Equipment transfer and return
c. Records transfer and return
d. Software implementation
e. Staffing designations for on-site and field support

C.8.9.5 Transition Out. The transition plan shall mitigate risks associated with a transition of services at the end of the task order period. The plan shall document the transition of powers, duties, activities, and functions of tasks and services for this task order. Upon conclusion of the task order, all records will be provided to CSOSA. The Contractor shall propose a plan that shall include, but not be limited to:

a. Specific Contractor needs from CSOSA to successfully transition away from location tracking system.
b. Provide contact information of the project manager appointed to coordinate the transition.
c. Process for CSOSA to request and receive monitoring uncertified and certified data, interpretation, and reports.
d. Process for providing court testimony at the end of the task order to include costs and information needed from CSOSA.

C.9 Reporting Requirements. Reporting requirements are listed in F.9.

C.10 Contractor Meetings

C.10.1 The Contractor will meet with the CO, COR, and other CSOSA personnel weekly during the first month after purchase order award. Meetings will occur on an agreed upon schedule monthly thereafter, or more often as deemed necessary in special circumstances. The Contractor will prepare meeting minutes and will distribute them to the attendees after each meeting. Meetings will be held virtually via teleconference and/or in a CSOSA office located within the Washington, DC, Metropolitan Area.

C.10.2 **Post-Award Meeting.** The Contractor shall participate in a post-award meeting scheduled by the COR to review the purchase order goals and objectives. This post-award meeting will take place no later than 10 days following the purchase order award.

C.11 Quality Assurance Protocol (QAP). The Contractor shall develop and provide to the CO within 10 days of purchase order award, a QAP that identifies what actions, processes, procedures, inspections, reviews, and responsibility assignments the Contractor will utilize to ensure that the Contractor's performance complies with all of the requirements of this purchase order. The CO shall have ten business days to review the QAP and provide requested or required changes to the Contractor. The Contractor will then have five business days to incorporate the CO's required/requested changes and return a final QAP to the CO. The Contractor's QAP shall be reviewed and updated as required, but no less than annually.

C.12 Inspections, Compliance & Audit

CSOSA through the CO, COR, or other CSOSA components shall conduct inspections and audits (hereafter "audit") to verify the personnel, operations, programs and the related non-financial books, records, accounts and information (including electronic data) of Contractor, comply with the provisions of this purchase order, or to assess the efficacy of any goods or services delivered pursuant to this purchase order. Contractor and its personnel shall cooperate fully with all audits.

C.12.1 Frequency of Audits. Audits shall occur at least once a year at the discretion of CSOSA. CSOSA retains the right to conduct audits more frequently if concerns about performance of the purchase order or the quality of the provided goods or services arise. CSOSA also retains the right to forgo an audit at its discretion and consistent with the Agency's policies and practices, or any applicable laws or regulations. Notwithstanding the foregoing, CSOSA and its representatives shall have the right to audit the Contractor at any time without notice and in addition to any annual audit, if there are concerns about fraud, waste, abuse, or mismanagement under the purchase order, or CSOSA has reason to believe that services procured through this purchase order are not being performed or are not meeting CSOSA's standards and expectations.

C.12.2 Personnel, Books and Records. Contractor shall keep full, true and accurate books, records, accounts and information (including electronic data) concerning services provided pursuant to this purchase order. Contractor shall comply with all reasonable requests of CSOSA or its representatives and provide access to all personnel, books, records, accounts and information (in whatever form, including electronic data) necessary for the audit, which may include, but not be limited to:

a. Offender files.
b. Notes and Reports (e.g., progress notes and discharge summaries).
c. Handbooks, manuals, policies and guidance for staff and offenders.
d. Outline of all offered services.
e. Staff position descriptions.
f. Organizational charts.
g. Agreements with external vendors or sub-contractors for services provided pursuant to the purchase order.
h. Proof of liability and other insurance.

i. Inspection Reports (e.g., environmental, facility).

C.12.3 Timing of Audits. Audits may be announced or unannounced at CSOSA's discretion and shall take place during Contractor's normal business hours. CSOSA and its representatives shall take reasonable steps to avoid disrupting the business of Contractor during an audit.

C.12.4 Audit Reports. Reports of the results of an audit are the property of CSOSA, but may be shared with Contractor at CSOSA's discretion. If deficiencies are observed during an audit, the CO shall issue a Corrective Action Report (CAR) to Contractor within five business days of being provided with deficiency information. The CAR shall identify the specific deficiencies and the timeframe in which Contractor shall take corrective action. Within five business days of receiving the CAR, Contractor shall develop and send to the CO for approval, a written plan of action with milestones (POAM) to correct the deficiencies within the timeframe designated by the CO. Contractor shall provide proof of remediation in writing to the CO for each deficiency identified in the CAR. Contractor may be subject to further audit by CSOSA to ensure that the corrective action taken is sufficient to prevent the reoccurrence of the deficiency.

C.12.5 Scope of Audit. CSOSA expects 100% compliance with the terms of this purchase order. The scope of the audit shall include, but is not limited to, the Statement of Work and other applicable sections of this purchase order; criteria identified in Contractor's QAP; standards issued by any accrediting body; Contractor's policies; and all applicable laws and regulations.

C.13 CSOSA Contractor Information Security Requirements

C.13.1 The Contractor shall meet and comply with Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, as amended and extended, for the protection of the information system and information during processing, while in storage, and during transmission. The Contractor shall be required to comply with, at a minimum:

a. Federal Information Security Modernization Act of 2014 (FISMA)
b. Office of Management and Budget (OMB) Circular and Memoranda (e.g. Circular A-130)
c. U.S. Department of Homeland Security Directives (e.g. US-CERT and HSPD-12)
d. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publication (SP) 800 Series (e.g. FIPS 200, FIPS 199, FIPS 140-2, SP 800-18, SP 800-37, SP 800-53A, SP 800-60)

C.13.2 The *Federal Information Security Modernization Act of 2014* (FISMA) requires the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information. It requires those measures to be in place for information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

a. The law defines the term "information security" to mean protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

    1. Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

    2. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

    3. Availability, which means ensuring timely and reliable access to and use of information.

b. The Contractor shall provide and implement security controls, as selected by CSOSA, to meet the security requirements for a Moderate impact level system as defined in NIST SP 800-53 (as amended), Security and Privacy Controls for Federal Information Systems and Organizations.

c. Executive departments and agencies procuring commercial and non-commercial cloud services, or systems provided or managed by other departments or agencies, contractors, or other sources shall comply with FISMA requirements. The Federal Risk and Authorization Management Program (Fed RAMP) is a government-wide program that provides a standardized approach to FISMA compliance as it applies to cloud-based computing services. It oversees and standardizes how to do security assessments, authorizations, and continuous monitoring for cloud products and services. Fed RAMP requirements apply to all cloud deployment models (e.g., Public Clouds, Community Clouds, Private Clouds, Hybrid Clouds); and all cloud service models (e.g., Infrastructure as a Service, Platform as a Service, Software as a Service) as defined by the National Institute of Standards and Technology (NIST).

C.13.3 Security Assessment and Authorization, and Continuous Monitoring. The Contractor shall apply the appropriate set of baseline security controls as required in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations*.

a. The Contractor shall be responsible for the cost of preparing the Security Authorization Package using NIST *SP 800-37* (as amended) *Guide for Applying the Risk Management Framework to Federal Information Systems* (using Fed RAMP templates, where available) and maintaining compliance.

b. The Contractor shall be able to maintain a security management continuous monitoring environment that meets or exceeds the *Continuous Monitoring* requirements in SP 800-37, Appendix G.

C.13.4 Requirements for Externally Hosted Services and Applications. Since the Contractor's CMS is external to CSOSA the following requirements also apply:

a. CSOSA reserves the right to perform Penetration Testing. If CSOSA exercises this right, the Contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with Fed RAMP requirements. Review activities include but are not limited to scanning operating systems , web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

b. Identified gaps between required Security Controls and the Contractor's implementation as documented in the System Security Plan (SSP) shall be tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document.

c. The Contractor is responsible for mitigating all security risks found during security assessment and accreditation and continuous monitoring activities. All high-risk vulnerabilities shall be mitigated within 30 days and all moderate risk vulnerabilities shall be mitigated within 90 days from the date vulnerabilities are formally identified.

d. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance. CSOSA reserves the right to conduct onsite inspections. The Contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

e. CSOSA has the right to perform manual or automated audits, scans, reviews, or other inspections of the Contractor's Information Technology (IT) environment being used to provide or facilitate services for CSOSA. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, the Contractor shall be responsible for the following security safeguards:

   1. The Contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this purchase order or otherwise provided by CSOSA.
   2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford CSOSA access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include, but is not limited to:
      i. Authenticated and unauthenticated operating system/network vulnerability scans;
      ii. Authenticated and unauthenticated web application vulnerability scans;
      iii. Authenticated and unauthenticated database application vulnerability scans; and
      iv. Automated scans can be performed by Government personnel, or agents acting on behalf of CSOSA, using Government operated equipment, and Government specified tools
   3. If new or unanticipated threats or hazards are discovered by either CSOSA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

f. If the Contractor chooses to run its own automated scans or audits, results from these scans may, at CSOSA's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by CSOSA. In addition, the results of Contractor-conducted scans shall be provided, in full, to CSOSA.

g. CSOSA may choose to cancel for convenience the (Contract/Award) if the Contractor has its authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

h. The Contractor shall comply with CSOSA security and privacy requirements (subject to change by the CSOSA Information Security Office) and as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement.

i. The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this purchase order.

j. The Contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this purchase order should be considered as Controlled Unclassified Information (CUI). It is anticipated that this information will be gathered, created, and stored within the primary work location. If Contractor personnel shall remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets.

k. CSOSA shall retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on Contractor's infrastructure, as well as maintains the right to request full copies of these at any time.

l. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure. The data shall be available to CSOSA upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein.

m. The Contractor shall provide requested data at no additional cost to CSOSA. No data shall be released by the Contractor without the consent of CSOSA in writing. All requests for release shall be submitted in writing to the CO.

n. The Contractor shall provide full access and cooperation for all activities determined by CSOSA to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of cyber incidents.

o. The Contractor shall be responsible for all costs and related resource allocations required for all subsequent incident response activities determined to be required by CSOSA, whether incurred by Government, agents under purchase order or on assignment to CSOSA, or by third party firms.

C.13.5 Additional Requirements for CSP hosted Services and Applications. If the Contractor's CMS is hosted in a commercial cloud service provider (CSP) environment like MS Azure, Amazon Web Services (AWS), IBM Cloud, Google Cloud, or similar the following requirements apply. The preferred level of Fed RAMP compliance status is moderate.

a. The Contractor shall implement the controls contained within the *Fed RAMP Security Controls Baseline*, and *Fed RAMP Continuous Monitoring Strategy Guide* available at the Fed RAMP website https://www.fedramp.gov/documents. These documents define requirements for compliance to meet minimum Federal information security requirements.

b. The Contractor shall follow Fed RAMP guidelines and security guidance. In situations where there are no procedural guides, the Contractor shall use generally accepted industry best practices for information security.

c. The Contractor shall be responsible for the cost of preparing the *Security Authorization Package* using the *Fed RAMP Security Assessment Framework* (SAF) process (using Fed RAMP templates, where available) and maintaining compliance.

d. The Contractor shall be responsible for preparing the Security Authorization Package using the Fed RAMP SAF Process and Fed RAMP Security Control Baseline Workbook.

e. The Contractor shall comply with Fed RAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement.

f. The Contractor shall create, maintain and update the documentation using Fed RAMP requirements and templates, which are available at https://www.fedramp.gov/templates/.

g. The Contractor shall use an accredited Third-Party Assessment Organization (3PAO) whenever there is a significant change to the system's security posture in accordance with the Fed RAMP Continuous Monitoring Strategy Guide.

h. To the extent required to carry out the Fed RAMP Security Assessment and Authorization (SA&A) Process (also known as the *Federal Risk and Authorization Management Program*) and Fed RAMP Continuous Monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford CSOSA access to the

Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

i. If new or unanticipated threats or hazards are discovered by either CSOSA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

C.14 Confidential Treatment of Sensitive Information.

C.14.1 The Contractor shall guarantee strict confidentiality of the information/data that it is provided by CSOSA during the performance of the purchase order. CSOSA has determined that the information/data that the Contractor will be provided during the performance of the purchase order is of a sensitive nature. The Contractor and its subcontractors performing under this PWS shall not copy, release, publish, or disclose non-public Agency information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of such information:

a. The Federal Acquisition Regulations (FAR)
b. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
c. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
d. 5 U.S.C. 552a (Privacy Act of 1974)
e. Public Law 96-511 (Paperwork Reduction Act)
f. Public Law 104-191, 110 Stat 1936 (HIPAA, The Health Insurance Portability and Accountability Act of 1996)
g. Public Law 107-204, 116 Stat 745 (SOX, The Sarbanes-Oxley Act of 2002)

C.14.2 Disclosure of the information/data, in whole or in part, by the Contractor can only be made after receiving prior written approval from the CO. Whenever the Contractor is uncertain with regard to the proper handling of information/data under the purchase order, the Contractor shall obtain a written determination from the CO.

C.14.3 Sensitive Information is any information, which if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, CSOSA, or CSOSA's interests. Sensitive Information is subject to stricter handling requirements because of the increased risk if the data are compromised. Some categories of Sensitive Information include Financial, Medical or Health, Substance Use, Legal, Strategic and Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as standalone information and may require additional protection in aggregate.

C.15 Section 508 Compliance. The system shall conform to the technical standards put forth in section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). and the U.S. Access Board’s Revised Section 508 Standards, effective January 18, 2018. These standards incorporate the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA requirements for digital content. Section 508 requires that when "Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.