TSP Digital Incident Reporting Technical Specifications

1. **Records Management System (RMS)**
    a. Software must be a web-based end user access with vendor being responsible for both primary and backup servers.
    b. The disaster-recovery server must be housed in excess of 300 miles from primary server.
    c. Vendor must be an approved/authorized entity to be able to electronically submit Tennessee Incident Based Reporting System (TIBRS) reports to Tennessee Bureau of Investigation.
    d. Software must be able to incorporate TIBRS required data fields as entries are made. These fields must be updated as TIBRS requirements change.
    e. Software must include all TIBRS required Tennessee Code Annotated offenses fields as well as the ability to enter other incidents that are area park related.
    f. System must contain the following components:
    Master name indexing **(See Item #2)**
    Master vehicle indexing **(See Item #6)**
    Arrest reporting **(See Item #3)**
    Inventory control such as evidence tracking
    Patient care reporting **(See Item #4)**
    Citation indexing that will track fees assessed, tendered, and past due **(See Item #5)**
    g. All modules must be integrated with all other system components requested in f. Each of these modules must be created, supported, and maintained by the same vendor to ensure consistency among modules and ease of support/maintenance for this agency
    h. Based on a user's login security, defined by the System Administrator, the system limits the capability to access and print incident reports that are not marked as more sensitive than the user's login security will allow. For instance, a juvenile-related report may be marked as highly sensitive and require a higher security level to access or print. Each user's security level will determine whether they have sufficient clearance to access or print a report.
    i. Software must allow import of Tennessee's Integrated Traffic Analysis Network (TITAN) Citation and Accident data into the Records Management System module for in-house data reference and the ability to provide historical search and link functionality. **(See Item #5)**

2. **Master Name Indexing (MNI)**

    a. MNI must permit the entry and query of an unlimited number of the following:
        - Physical description history
        - Aliases/AKAs
        - Associates
        - Employer Information

b. MNI must allow for multiple entries and queries when necessary of the following data elements:
    - Last name
    - First Name
    - Middle name
    - Suffix
    - Date of birth
    - Social Security number
    - Driver's License/ID number and state
    - Address
    - Phone Number
    - Height
    - Weight
    - Address History
    - Hair Color, length, style
    - Eye Color
    - Facial Hair
    - Sexual Orientation
    - Complexion
    - Body Markings (scars, tattoos, etc.)

c. This system must also allow the operator to inquire into names in the system using many combinations of search criteria, including: Partial name, AKAs, Street Name, Social security number, Date of birth, Sex, Race, Hair color, Eye color, Height, Weight, Scars/marks/tattoos.
d. Access to MNI information from other file systems is interactive, i.e. during edit/entry of an incident; the user is not required to exit from other modules to enter MNI information and does not require exit from the module to search a name record.
e. To prevent duplication of entries, a data entry safeguard must be in place to perform an automatic check against existing MNI data.
f. Must have an evidence entry and storage functionality in the software. This includes various types of evidence and the ability to upload files, photos, and videos. The attachment single file size allowable up to 800gb.
g. The software must have the ability to assign a specified "report number" sequence based on each park and region's Originating Agency Identifier (OIR) number.
h. A narrative field will need to allow an unlimited number of character entries.
i. The software must allow an approval process after each Ranger/Manager enters a report.
j. The State must be able to control the hierarchy of approval steps.
k. The software must be able to have various searchable fields for "batch reporting." Supervisors must be able to enter specific fields for all incidents that occurred by
park or in all 56 parks.

3. **Arrest Report Module (ARM)**
    a. ARM must track all persons arrested and be linked to the RMS module via the case/incident number.
    b. ARM must have all elements in order to be TIBRS compliant.
    c. ARM must produce a Criminal History Report (Rap Sheet).
    d. ARM must produce reports of arrest by:
        - Charge
        - Location/Park/Region
        - Date/Time Ranges
        - Ranger/Manager
        - Disposition
    e. ARM must have the capability to store a lengthy amount of narrative information.

4. **Patient Care Report Module (PCRM)**
    a. PCRM module must be HIPAA compliant with all information entered into the data base. The required data fields can be supplied to vendor.
    b. PCRM must utilize the same "master name indexing" function of the RMS module to reduce redundant data entry and ensure accuracy.
    c. PCRM must have a supervisor approval hierarchy like the RMS system.
    d. Once the final supervisor approves, must have the ability to send to the agency's medical director for review and approval.
    e. Access to PCRM will need to be limited to only authorized users.

5. **Accident/Citation Tracking Module (ACTM)**
    a. ACTM will track all accidents and or citations issued.
    b. Crash/Accident data will need to be imported from TITAN on a set frequency to RMS.
    c. ACTM must be able to track accidents and or citations by location to ensure they are recorded at the park where they occur and/or are issued.
    d. ACTM must also link to the MNI function of the RMS module to provide linked data by a person's name.
    e. ACTM must track fees assessed to each citation, payments received, and past due amounts.
    f. ACTM must also have an "Access Only" feature to allow non-law enforcement personnel access to query citations that have been issued, payment entries, and past due status.

6. **Motor Vehicle Indexing (MVI)**
    a. The MVI must contain each of the following data elements and allow inquiry into the MVI under many combinations of the data elements:
        - Type
        - Year
        - Make
        - Model
        - Style

- Color
- Other descriptors, characteristics, etc.
- Owner
- Operator
- License plate and state
- License year
- Vehicle identification number

b. MVI must accommodate all types of vehicles, including cars, trucks, motorcycles, ATV's and boats and provide a field for indicating the type.
c. MVI must provide features to help the agency avoid duplicate entry of information for the same vehicle.
d. Entry of a vehicle owner's name must invoke a check of the MNI system with this vehicle being associated the name in MNI.
e. MVI must allow linking of vehicle information to the owner and applicable incidents, crashes, and citations.

7. Service Provider Hosted Services, Confidential Data, Audit, and Other Requirements.

a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:

(1) The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.

(2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.

(3) The Contractor and the Contractor's processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO") 27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants ("AICPA") for a System and Organization Controls for service organizations ("SOC") Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification or FedRAMP authorization for the Contractor and Subcontractor(s), or provide the State with the Contractor's and Subcontractor's annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.

If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor's opinion in the most recent audit report.

No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.

(4) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Processing Environment.

(5) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State

(6) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

b. Minimum Requirements

(1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the State's Enterprise Information Security Policies as amended periodically. The State's Enterprise Information Security Policies document is found at the following URL: https://www.tn.gov/finance/strategic-technology-solutions/strategic-technology-solutions/sts-security-policies.html.

(2) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

(3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.

c. Comptroller Audit Requirements

Upon reasonable notice and at any reasonable time, the Contractor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Contract. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit.

The information technology control audit may include a review of general controls and application controls. General controls are the policies and procedures that apply to all or a large segment of the Contractor's or Subcontractor's information systems and applications and include controls over security management, access controls, configuration management, segregation of duties, and contingency planning. Application controls are directly related to the application and help ensure that transactions are complete, accurate, valid, confidential, and available. The audit shall include the Contractor's and Subcontractor's compliance with the State's Enterprise Information Security Policies and all applicable requirements, laws, regulations or policies.

The audit may include interviews with technical and management personnel, physical inspection of controls, and review of paper or electronic documentation.

For any audit issues identified, the Contractor and Subcontractor(s) shall provide a corrective action plan to the State within 30 days from the Contractor or Subcontractor receiving the audit report.

Each party shall bear its own expenses incurred while conducting the information technology controls audit.

d. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:

(1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:

i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: [5 minutes]
ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: [1 hour]

(2) The Contractor shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

e. Personally Identifiable Information.

(1) While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to:
(i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and
(ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the

purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify or ensure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law. The obligations set forth in this Section shall survive the termination of this Contract.