

**State of Tennessee
Specifications
Sourcing Event # 9160**

Finance and Administration, Office for Information Resources

SCOPE:

This solution must include the following services of ServiceNow's IT Service Management Solution as defined by Gartner:

Help Desk and Problem Management,
Change Management,
Asset and Configuration Management-CMDB,
Repository for Asset Management
Service Catalog,
Request Fulfillment,
Service Level Management,
Knowledge Management
Associated reporting and dashboards.

- A.1. The Contractor shall provide a methodology for defining Service Level Agreements and Organizational Level Agreements on all event types (Incident, Change, Work Order, Task, etc.) configurable at the agency/division level.
- A.2. The Contractor shall provide a methodology for defining and managing configuration / asset items (hardware, software, etc.).
- A.3. The Contractor shall provide an asset module that is a part of a fully configurable CMDB.
- A.4. The asset module will have the ability to define and configure configuration business modeling and mapping.
- A.5. The Contractor shall provide Full Asset Management capability.
- A.6. The application has the ability to manage software licensing and contracts in order to maintain compliance within the organization.
- A.7. The Contractor shall authenticate with LDAP.
- A.8. The Contractor shall have the Ability to Integrate with a web service.
- A.9. The Contractor shall provide a configurable, intuitive and consistent system experience to our customer that is easy to brand as necessary.
- A.10. The Contractor shall provide for role based security, up to the field level if necessary, to control system access and usage by our Customers.
- A.11. The Contractor shall provide for an internal / local password login when necessary and have an easily configurable password policy (length, content, expiry, etc.) to ensure compliance with state security policies.
- A.12. The solution shall have the ability to easily configure all data entry fields within the layout of a module with no coding required, nor should configurations cause any loss or increase in cost to technical support.

- A.13. The Contractor shall provide a configurable dashboard with a wizard based designer and requires no scripting.
- A.14. The application must be compatible with State Standard browser applications. (currently IE versions 9, 10 & 11) as well as browsers that the State may use (Firefox, Chrome, Opera, Safari, etc.).
- A.15. Transaction Response Time - 95% of all transactions will complete within one second, and no single transaction may exceed 5 seconds.
- A.16. The solution shall provide a means of accessing the system via a multitude of mobile devices using iOS 6.0 or higher, Android 4.4 or higher and Windows 8.1 or higher.
- A.17. The application must have a built-in reporting console with the ability to generate a report with fields from related tables without the need for vendor customization.
- A.18. The solution shall contain both a series of pre-defined dashboards and standardized reports but allow for easy generation of any needed ad-hoc reporting.
- A.19. The Contractor shall provide Agency specific reports and dashboards that will only be accessible by the specific agency responsible
- A.20. Asset management must store all owned assets of NetTN.
- A.21. All System security shall be compatible with TN Enterprise Information Security Policies. The Policy, as may be periodically revised, can be located at the following link:
https://www.tn.gov/assets/entities/finance/oir/attachments/PUBLIC-Enterprise-Information-Security-Policies-v2.0_1.pdf
- A.22. The solution shall be Compliant with NIST Special Publication 800-53, Revision 3 - Recommended Security Controls for Federal Information Systems and Organizations (as amended)
- A.23. Tennessee will own all rights, title and interest in its data. The contractor will comply with all rights and requests for data by the state and will not use the data except as authorized.
- A.24. All data at all times will remain within the Continental U.S.
- A.25. All data will be encrypted at rest and in transit in accordance with FIPS PUB 140-2. The State will hold all encryption keys.
- A.26. Contractor will provide four separate operating environments will be included – Development, Testing, Disaster Recovery and Production - must mirror in functionality and features.
- A.27. System will be available 99.8 % of the time including scheduled maintenance. Scheduled maintenance will be defined in the contract and will be performed at mutually agreeable times.
- A.28. There will be complete Business Continuity and Disaster Recovery plans that ensures that the Recovery Point Objective of one hour and recovery time objective of 2 hours are met
- A.29. Vendor is certified, accredited and audited on a yearly basis to validate security through SOC 2 Type 2 and ISO 27001. Vendor will provide certificates and audit results to the State on an annual basis.
- A.30. The solution shall have defined and documented Incident and breach response in accordance with TN Enterprise Information Security Policies and State Law as outlined in the Tennessee Code Annotated (TCA).
- A.31. The solution shall have multifactor authentication.

- A.32. The solution shall have defined and documented security standards to ensure data is secure and safe from intrusion.
- A.33. The solution shall provide Incident and Problem Management - The ability to manage the life cycles of IT incidents and problem records from recording to closing. The solution should support the collection, analysis and communication of incident and problem management data.
- A.34. The solution shall provide Change, Configuration and Release Management — The ability to govern various aspects of the IT change management process. The tool must also support the configuration management process by enabling the creation and maintenance of a complete and accurate picture of configuration across various infrastructure elements via a CMDB. Lastly, the tool must provide release governance capabilities to ensure that approved changes are executed in the environment in accordance with the IT organization's defined and documented procedures.
- A.35. The solution shall provide Service Request Management — The ability to present an online portal to business end users who are requesting help from the IT service support organization in the forms of incident reports, change requests, IT component ordering or administration.
- A.36. The solution shall provide IT Knowledge Management - The ability to collect, store and access information about IT services to enable the infrastructure and operations organization to better manage IT service assets through their life cycles. The service knowledge portal should enable user self-service so that end users may resolve simple incidents themselves.
- A.37. The solution shall provide Reporting and Dashboards - the ability to provide trend reports that measure operational productivity across core processes. Dashboard and reporting capabilities must be tied to business value metrics, common critical success factors and key performance indicators. The tool must offer multidimensional charts that show how related metrics affect each other.
- A.38. The solution shall provide Out-of-the-box best practices - the quality of preconfigured workflows in accordance with industry best practices and the ease of use with respect to modifying those workflows as needed.
- A.39. The Contractor shall document a Training Strategy that outlines their approach for training State Entities during the Transition-in project. The Training Strategy will outline the specifics of how training needs will be identified and training artifacts will be designed, developed and delivered. The goal is to provide a training program that will prepare Entities to be fully operational when the transition is complete.
- A.40. The Contractor will develop and maintain content, in conjunction with OIR, using the State-approved Branding Standards that are visually appealing and provides a consistent “look and feel,” as determined by the State (navigation, page layout, features and functionality)
- A.41. The Contractor must comply with industry best practices in the provision of services under this Contract.
- A.42. Upon Termination of Contract and at the State’s request, the Contractor will, in all practical and contractually allowable cases, transfer all data to the State that is necessary to continue the successful operation and maintenance of the services by the State. This data shall remain available to the State to transfer for a period of time the State deems reasonable to transfer the data.
- A.43. When requested by the State designee, at the termination of the contract, Contractor will destroy all hard copies of State’s data and sanitize/wipe all digital copies. The Contractor shall provide proof to the State that this was done.
- A.44. Contractor represents and warrants that the term of the warranty (“Warranty Period”) shall be the greater of the Term of this Contract or any other warranty general offered by Contractor, its

suppliers, or manufacturers to the States of its goods or services. The goods or services provided under this Contract shall conform to the terms and conditions of this Contract throughout the Warranty Period. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge.

Contractor represents and warrants that the State is authorized to possess and use all equipment, materials, software, and deliverables provided under this Contract.

Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor's industry.

If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services. Any exercise of the State's rights under this Section shall not prejudice the State's rights to seek any other remedies available under this Contract or applicable law.

Contractor shall provide to the State all software upgrades, modifications, bug fixes, or other improvements in its software that it makes generally available to its other customers.

A.45. The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any defects, the goods or services shall be deemed to have been accepted by the State.

A.46. The Contractor shall assure that the environment content and applications are compliant with **applicable** standards, laws, and regulation (see below):

Federal Information Security Management Act (FISMA);

NIST Special Publication 800-53, Revision 3 - Recommended Security Controls for Federal Information Systems and Organizations (as amended);

ISO27001 (International Standard for an information security management system);

System Organization Control 2 (SOC 2);

Health Insurance Portability & Accountability Act (HIPAA);

Health Information Technology for Economic and Clinical Health (HITECH);

Personally Identifiable Information (PII);

The Contractor shall make relevant audit or certification reports available for State review upon request.

As additional State and Federal Security and Regulatory requirements are imposed, the Contractor shall ensure that the environment content and applications are kept up to date with the emerging requirements.

A.47. SaaS Services refers to the collection of online web-based business application software hosted and provided by the Contractor.

The Contractor may update the content, functionality and user interface thereof with error corrections, improvements and other modifications from time to time at its discretion and at no additional cost to the State. The Contractor additionally will make available to the State the online user manuals, as updated from time to time, that describe the functions, operation, and use of the SaaS Services.

During the term of this Contract, the SaaS Services will perform materially in accordance with the documentation, and the functionality of the SaaS Services will not be materially decreased from that available as of the beginning of the Contract Period.

- A.48. The Contractor is responsible for securing the technical environment from unauthorized access or exploits by employing all measures and controls deemed reasonable and appropriate by industry accepted best practices. Authorized access is limited to State Users and to those persons authorized by the Contractor for the purpose of carrying out work in support of this Contract. The technical environment includes that environment accessed by State Users for the purpose of making use of the SaaS Services, and/or any physical or virtual location where State Data is stored. State Data includes all pre-existing or electronic data or information submitted by the State in the process of making use of the SaaS Services. Further, all State Data, including data stored in databases and data backups will be stored on-shore within the United States of America.

The Contractor is also responsible for maintaining the environment's compliance with applicable technology standards as documented in the Tennessee Technology Architecture – Standard Products document. Generally, applicable technology standards include, although not limited to, those standards related to:

The operating systems for the desktop and mobile devices used to access the technical environment,

The web browsers used to access the SaaS Services,

The personal computing applications (E.G., Microsoft Word and Excel, Adobe Acrobat, etc.) used to prepare documents and other files to be saved in the technical environment, and

Other technologies, the applicability of which arises as a result of the work conducted under a Statement of Work (E.G., identity federation).

The availability target for the SaaS Services is twenty-four (24) hours per day, seven (7) days per week, with allowance for pre-planned times of unavailability necessary for the Contractor to perform regularly scheduled maintenance. The Contractor will provide its plan for regularly scheduled maintenance to the State on a quarterly basis. For all unscheduled maintenance that will result in unavailability (I.E., not regularly scheduled maintenance), the Contractor will make reasonable effort to provide the State a minimum of seven days advance notification. All reasonable effort will be made by Contractor to schedule periods of unavailability (scheduled and unscheduled) during non-peak work hours (I.E., Monday through Friday, between 6:00 PM and 6:00 AM CST/CDT or on weekends).

- A.49. The Contractor will provide all service described in the Contract and Statement of Work to the State at no additional cost. All prices must include travel expenses. The State will not sign any Statement of Work's.
- A.50. The Contractor will establish and set up the technical environment for the State's use. The Contractor will further configure the component solutions within the SaaS Services as specified in and through the conduct of work under the relevant Statement of Work executed. Additionally, the Contractor will system test such configurations to confirm that they appropriately meet the agreed to, in scope capabilities and provide appropriate response times, as specified in and through the conduct of work under the relevant Statement of Work executed.

- A.51. The Contractor will provide assistance to the State to accomplish the integration of the applicable component of the technical environment with other State owned technology assets.
- A.52. The Contractor will provide consulting services to the State for the purpose of implementing and configuring the components of the SaaS Services. Consulting services will also be provided for the purpose of integrating the SaaS Services with other State owned technology assets as described. Specification of implementation, configuration and integration requirements will be as requested and accomplished through the execution of a Statement of Work as described. The State will not sign any Statement of Work's.
- A.53. The Contractor will guarantee partial or total destruction of the data in its safekeeping, including mirrored and backup data, at the request of the state.
- A.54. The Contractor will utilize SAML/SSO capabilities for authentication.
- A.55. The Contractor will immediately disable access in the event of a breach.
- A.56. The State will be immediately notified in the event of important changes like security practices and regulations, changes in business model or data center locations.
- A.57. For end-of-life and failed storage devices contractor will follow NIST 800-88 standards for disk destruction and media sanitization. All end of life disks are stored in a safe inside the data center cage until they can be shredded. Proof of destruction will be provided to the State.
- A.58. For all legal hold requests contractor will clone the instance and leave it inactive. This hardware will be held and preserved forever.
- A.59. The Contractor shall provide 24 hour support under the standard maintenance program (e.g., phone support, online support, fixes, compliance updates, and enhancements).
- A.60. The contractor will provide appropriate access control to restrict access to only approved State users.
- A.61. All servers and network devices will have fully replicated redundant components and multiple network paths, to avoid single points of failure and loss of data.
- A.62. All employees with access to State equipment and data shall be fully screened with criminal history checks and background checks in accordance with NIST Special Publication 800-53, Revision 3 - Recommended Security Controls for Federal Information Systems and Organizations (as amended) guidelines.
- A.63. The Contractor shall provide to the State on a quarterly basis, the results of all network and application vulnerability assessments and data center inspections.
- A.64. When laws or regulations change they will automatically become part of this Contract.
- A.65. Contractor represents and warrants that the term of the warranty shall be the greater of the Term of this Contract or any other warranty general offered by Contractor, its suppliers, or manufacturers to the States of its goods or services. The goods or services provided under this Contract shall conform to the terms and conditions of this Contract throughout the Warranty Period. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a "Defect" and shall be considered "Defective." If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge.

Contractor represents and warrants that the State is authorized to possess and use all equipment, materials, software, and deliverables provided under this Contract.

Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor's industry.

If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services. Any exercise of the State's rights under this Section shall not prejudice the State's rights to seek any other remedies available under this Contract or applicable law.

- A.66. The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.
- A.67. Subject to the terms of this Contract, the State may access and use the purchased Subscription Service during the Subscription Term as set forth in this contract for its internal business purposes in accordance with the documentation. The State shall not use or otherwise access the Subscription Service in a manner that exceeds the State's authorized use as set forth in this Contract.
- A.68. Contractor grants the State a limited, personal, worldwide, non-sub-licensable, non-transferable, non-exclusive license during the Subscription Term to install and execute Software on machines operated by or for the State solely to facilitate State's authorized access to and use of the purchased Subscription Service. The Software may include code that is licensed under third party license agreements, including open source made available or provided with the Software. Software is licensed and not sold even if for convenience Contractor makes reference to words such as sale or purchase.
- A.69. As between Contractor and the State, all rights, title, and interest in and to all intellectual property rights in the Contractor Core Technology are owned exclusively by Contractor notwithstanding any other provision in this Contract. Except as expressly provided in this Contract, Contractor reserves all rights in the Contractor Core Technology and does not grant the State any rights, express or implied or by estoppel.
- A.70. As between the State and Contractor, the State shall retain all of its rights, title, and interest in and to its intellectual property rights in the State Data and the State Technology. The State hereby grants to Contractor a royalty-free, fully-paid, non-exclusive, non-transferable sub-licensable, worldwide right to use the State Data and the State Technology solely for the purpose of providing the Subscription Service and Professional Services to the State.
- A.71. Contractor warrants that during the Subscription Term, the State's instances of the Subscription Service shall materially conform to the Product Overview.
- A.72. Upon termination of the Subscription Service for any reason, the State shall stop using, and Contractor shall stop providing, the Subscription Service and all rights granted to the State in this Contract shall terminate. Contractor shall within thirty (30) days following the effective date of a termination by the State for Contractor's breach refund to the State all prepaid fees received by Contractor covering the remaining portion of the Subscription Term for the affected Subscription Service after the date of the termination.
- A.73. At least thirty (30) days prior to either the expiration of the Subscription Term (where the State elects not to renew) or in connection with the termination by the State of the Subscription Service, the State may purchase the following services: (i) one (1) extension of the Subscription Service for up to six (6) months ("Transition Subscription Service"); and (ii) Professional Services. The State shall pay in advance for the Transition Subscription Service at the monthly subscription fee

rate charged to the State in the expiring Order Form. The State shall pre-pay for any Professional Services ordered during the transition period. The parties shall agree in the Order Form the fees and purchased Subscription Service and Professional Services prior to the commencement of any Transition Subscription Service or Professional Services. The State's Purchase Order will be the binding document for the services listed on the Order Form. The State will not sign any Order Form.

- A.74 Contractor shall provide the State Data in its standard database export format, excluding the Contractor Core Technology, to the State upon the State's written request and at no additional cost to the State. After one hundred eighty (180) days following the expiration or termination of this Contract for the Subscription Service (including any Transition Subscription Service term, if applicable).
- A.75. **All services performed under this contract will be performed by ServiceNow and its employees, not those of any contractor.**
- A.76. **All customer service support, including Tier 1 support will be performed by ServiceNow and its employees.**
- A.77. **All services will be performed by ServiceNow and its employees in its data centers utilizing only ServiceNow controls and governance.**
- A.78 Contractor will be responsible to ensure all items in attached Appendix 1 ServiceNow Statement of Work (SOW) are completed by ServiceNow to the satisfaction of the State.
- A.79. **Contractor must be an Authorized ServiceNow Solution partner.**
- A.80. All instances must be **dedicated** State of TN instances within the ServiceNow infrastructure.
- A.81. **The State will not pay for any travel expenses associated with Professional Services and Training. All expenses must be included in bid price.**