State of Louisiana
Office of Technology Services

Request for Information (RFI) related to Commercially Available Configuration Management Database (CMDB) Solutions

RFI # 3000025021

This Request for Information (RFI) is for planning purposes only and should not be construed as a Request for Proposal (RFP). This is not a solicitation for offers. This information will be reviewed and discussed by the State agency and may result in the advertisement of a formal and competitive Request for Proposal or other procurement activity for the services included in the RFI.

Overview

Purpose of the Request for Information

The Office of Technology Services (OTS) is issuing this Request for Information (RFI) to solicit input from qualified vendors regarding commercially available Configuration Management Database (CMDB) solutions suitable for large, complex, and consolidated enterprise environments.

This RFI is intended to gather high-level, non-binding information on the current landscape of CMDB technologies, architectures, and implementation strategies that can support a robust, scalable, and secure configuration management capability across the enterprise. OTS seeks to understand how solutions address challenges such as multi-source configuration data reconciliation, real-time asset and relationship discovery, integration with IT service management (ITSM) and operations (ITOM) platforms, and support for hybrid (on-premise and cloud) infrastructures.

Objectives of the Request for Information

- Identifying leading CMDB solutions capable of meeting enterprise-scale requirements;
- Understanding architectural models, deployment options, and integration strategies;
- Gaining insight into automation, discovery, and data quality management features;
- Assessing vendor experience with public sector and/or large enterprise implementations;
- Evaluating emerging capabilities related to service mapping, observability, and AIOps;
- Understanding the relationships between CMDB and incident, problem, change, and release management processes;
- Understanding integrations with dependent processes (e.g. change, release) to automatically surface dependency impacts and risk scores.

Respondents are encouraged to share relevant documentation, deployment case studies, and product roadmaps that help illustrate their solution's maturity and alignment with the goals outlined herein.

RFI Coordinator

RFI responses must be directed to the RFI coordinator:

Matthew Vince
Office of Technology Services
P.O. Box 94095
Baton Rouge, LA 70804-9095
Phone: 225-342-7105
Fax: 225-219-9475
Email: pmo@la.gov

All communications relating to this RFI must be directed to the RFI Coordinator named above. All communications between respondents and State staff members, other than the RFI Coordinator, concerning this RFI are strictly prohibited. Inquiry emails should use the following subject line format: RFI #3000025021 – QUESTION – <Vendor Name>.

Schedule of Events

The State reserves the right to revise this Schedule of Events.

Event	Date	Time
Public Notice of RFI	6/16/2025	
Deadline for Receipt of Questions/Inquiries	6/23/2025	4:00 PM CT
Deadline for State's Response to Questions/Inquiries	6/25/2025	
Deadline for Receipt of RFI Responses	7/16/2025	4:00 PM CT

Response Preparation Cost

The State will not pay for the preparation of any information or response submitted in reference to this RFI, nor will it pay for any use of response information. The respondent assumes sole responsibility for any and all costs and incidental expenses associated with the preparation and

reproduction of any materials submitted in response to this RFI. This includes preparations for approved discussions, demonstrations, or vendor marketing materials.

RFI Addenda/Cancellation

The State reserves the right to revise any part of the RFI by issuing an addendum to the RFI at any time. Issuance of this RFI, or subsequent addendum (if any), does not constitute a commitment by the State to issue an RFP or any other process resulting in award of a contract of any type or form. In addition, the State may cancel this informal process at any time, without penalty or prior notice.

Proprietary and/or Confidential Information

Pursuant to the Louisiana Public Records Act (La. R.S. 44:1 et. seq.), all public proceedings, records, contracts, and other public documents relating to this RFI shall be open to public inspection. Respondents should refer to the Louisiana Public Records Act for further clarification, including protections sought for proprietary and/or trade secret information. Respondents are reminded that any material within a response to this RFI identified as confidential or proprietary must be clearly marked. Any response marked as confidential or proprietary in its entirety may be rejected without further consideration or recourse.

Written Inquiry/State Response Process

Respondents may submit written inquiries to the RFI Coordinator via email according to the Schedule of Events herein.

The State shall provide responses to all written inquiries, according to the Schedule of Events, in the form of an RFI addendum, posted to the LaPAC at https://wwwcfprd.doa.louisiana.gov/osp/lapac/pubMain.cfm.

Response Submission

All responses to this RFI must be received by the due date and time indicated on the Schedule of Events. Responses received after the due date and time will not be considered. It is the sole responsibility of each respondent to assure that its response is delivered at the specified

location prior to the deadline. Responses which, for any reason, are not so delivered will not be considered.

Electronic Submissions

Electronic submissions are the preferred format. Electronic submissions may be made using the Dropbox File Request system via the following link. Electronically submitted responses should be in Microsoft Word and/or PDF format.

https://www.dropbox.com/request/VJ2fJmvRIQaq9e2lQY86

No submissions will be accepted via email.

Hard Copy Submissions

Hard copy response submissions, which should include at least one (1) hard-copy and one (1) digital (flash drive) copy, may be submitted via the U.S. Mail, courier, or hand-delivered:

If courier mail or hand-delivered

Matthew Vince
Office of Technology Services
Claiborne Building
1201 N. 3rd Street, Suite 2-130
Baton Rouge, LA 70802

If delivered by U.S. Mail

Matthew Vince
Office of Technology Services
P.O. Box 94095
Baton Rouge, LA 70804-9095

Ownership of Responses

All materials submitted become the property of the State and will not be returned to the respondent. The State retains the right to use any and all ideas or adaptations of ideas contained in any response received through this RFI process.

Format of Response

All responses shall be submitted in hard-copy and digital format (PDF or Word is preferred), not to exceed 50 pages, in 10pt. font or larger according to the following outline:

Corporate Background and Experience
Responder shall provide a brief description of the company, including a brief history, corporate structure, and organization and the number of years in business.

Business Model for Contracting of Services
Responder shall describe its approach to a contract for its services should it be awarded a contract, but without providing any cost information in its response.

If a Commercial- Off-the-Shelf or Software-as-a-Service solution is proposed, the responder should indicate if proposed products are available through NASPO ValuePoint or similar purchasing agreements.

Approach and Methodology
Responder shall describe its proposed solution and approach for delivery of services, specifically identifying the use of delivery methodologies, or other methods to address evolving system needs.

Implementation Timeframe of Solution
Responder shall indicate the minimum time frame from contract execution for full implementation of its solution, inclusive of equipment acquisition, configuration, and testing.

No cost and/or marketing information shall be included in this RFI response.

Optional Discussion

To solicit feedback and ask follow-up questions based upon vendor RFI responses, The State reserves the right at their sole discretion to conduct a structured discussion for respondents to this RFI only. An agenda, specific questions and other expected topics for discussion may be provided prior to the discussion.

The State is not under any obligation to conduct discussions with any respondent to this RFI.

Scope of Services

Background

The Louisiana Office of Technology Services (OTS) is the centralized provider of IT infrastructure and services for executive branch agencies within the State of Louisiana. OTS is responsible for delivering secure, efficient, and standardized technology services across a diverse array of agencies and mission-critical functions. The IT environment under OTS management includes complex hybrid infrastructures, legacy and modernized systems, and a growing portfolio of cloud-based services.

As part of its enterprise modernization and IT service management (ITSM) initiatives, OTS has identified the need to establish a comprehensive, authoritative, and scalable Configuration Management Database (CMDB). The CMDB will serve as the foundation for improved operational visibility, service impact analysis, change risk assessment, incident resolution, and compliance auditing.

Currently, configuration and asset data is dispersed across multiple systems, including service desks, network discovery tools, endpoint management platforms, cloud consoles, and manually maintained documentation.

To address these items, OTS seeks to understand the current state of the market and available technologies that support:

- Automated and accurate discovery of configuration items (CIs) across hybrid environments;
- Work within complex and highly segmented network infrastructure;
- Integration with ITSM platforms (e.g., Ivanti, ServiceNow);
- Real-time CI relationship mapping and service modeling;
- Data reconciliation and lifecycle governance;
- Role-based access controls, audit trails, and compliance features.

Respondent Information

Respondents are requested to provide a comprehensive overview of their organization, experience, and operational capacity to support a Configuration Management Database (CMDB) solution suitable for large-scale enterprise and government environments. This section is intended to establish a baseline understanding of their organizational profile, past performance, product maturity, and long-term viability.

Respondents should include the following details:

Relevant Experience

- A summary of experience deploying CMDB solutions in large enterprise or public sector environments.
- List of at least three relevant reference customers (preferably government or regulated industry) including:
    - Agency or organization name,
    - Implementation size and scope,
    - Key use cases supported,
    - Contact information (if permissible).
- Experience integrating with common government IT ecosystems, such as Ivanti, ServiceNow, Microsoft MECM, Azure, AWS, or security, network, and application monitoring platforms.

Product and Support Information

- Overview of core product offerings relevant to CMDB, including any bundled or integrated modules (e.g., discovery, service mapping, AIOps).
- Product versioning strategy and release cadence.
- Support offerings including tiers, response time commitments, hours of operation, and escalation procedures.
- Training, onboarding, and documentation resources available to customers.
- Availability of U.S.-based or onshore support teams (if applicable for compliance or security requirements).

Certifications and Compliance

- Product and organizational certifications (e.g., ISO 27001, SOC 2, ITIL, FedRAMP, StateRAMP).
- Compliance with federal and state cybersecurity standards, including NIST SP 800-53 or state-specific requirements.
- Information on any data residency, encryption, and privacy policies relevant to U.S. state government customers.

System Functionality and Responsibilities

Respondents are requested to provide detailed information regarding the capabilities and responsibilities of their proposed CMDB solution in support of an enterprise-scale, hybrid IT environment. The system should act as a central source of truth for configuration data, while enabling extensibility, federation, and automation in alignment with ITIL best practices and modern IT operations (ITOM) frameworks.

The following subsections outline the required and expected areas of functionality. Respondents should address each area with specificity, including product features, configurable options, architectural approaches, and deployment considerations.

Respondents should clearly delineate between native functionality, configuration/customization options, and third-party dependencies. Where applicable, include diagrams, product screenshots, and references to public documentation or case studies demonstrating the requested capabilities in similarly sized environments.

Core CMDB Capabilities

- Ability to define, store, and manage Configuration Items (CIs) and their associated attributes, classifications, and states.
- Support for flexible, extensible CI classes and custom data models.
- Robust relationship modeling between CIs, including business services, applications, network and server infrastructure components, and cloud-native resources.
- Native support for lifecycle management of CIs, including state transitions, deprecation, and archival.
- Change versioning to track the full cycle of short-lived CIs.
- Support for streaming data processing and real-time updates to the CMDB.

Discovery and Data Ingestion

- Automated discovery of hardware, software, network, virtual, and cloud assets across on-premises, multi-cloud (e.g., AWS, Azure, GCP), and hybrid environments with complex, non-flat network architecture.
- Support for agent-based, agent-less, and API-based discovery methods.
- Continuous or scheduled scanning capabilities with conflict resolution and version tracking.

- Ingestion of data from external systems (e.g., SCCM, vCenter, identity platforms) with configurable connectors.
- Real-time or continuous, event-driven asset discovery and service dependency mapping, including ephemeral assets and cross-domain dependencies.

Data Quality and Reconciliation

- Mechanisms for deduplication, normalization, and validation of CI data.
- Multi-source data reconciliation with source-of-truth prioritization and audit trails.
- Policy-based enforcement of CI attribute completeness and accuracy.
- Support for reconciliation rules that can be customized to agency or system-specific requirements.

Integration and Interoperability

- Native or standards-based integrations with leading ITSM platforms (e.g., Ivanti, ServiceNow).
- Ability to consume and provide data to external CMDBs or federated repositories using open APIs or data federation frameworks.
- Integration with security tools (e.g., SIEM, SOAR, vulnerability scanners) and operational tools (e.g., APM, orchestration platforms).
- Event-driven data updates via webhooks, message queues, or real-time API calls.

Visualization and Service Mapping

- Dynamic visualization of relationships and dependencies among CIs, including service maps and dependency trees.
- Automated service modeling based on discovered application flows and communications.
- Impact analysis capabilities to assess the downstream effects of changes or outages.

Access Control, Security, and Compliance

- Role-based access controls (RBAC) with granular permissions on CI types, attributes, and actions.
- Support for data segmentation and tenant-aware CMDB capabilities, if applicable.
- Full audit logging of data access, modifications, imports, and deletions.

- Compliance with government security frameworks (e.g., NIST 800-53, FedRAMP, CJIS where applicable).

Administration and Maintenance

- Tools for system configuration, policy management, and operational health monitoring.
- Administrative dashboards for data quality, ingestion status, and reconciliation conflicts.
- Scheduling, alerting, and notification mechanisms for discovery and integration events.
- Maintenance window controls.
- Self-service functions.
- High Availability and Disaster Recovery features.

Appendices / Attachments

Please include any supporting documentation needed to support the response to this RFI. Some examples are listed below:

- Sanitized network diagrams
- Existing architecture standards or policies
- Example use cases or workflows
- Sample reports or dashboards
- Sample metrics or KPIs (e.g. change success rate, time to reconcile CIs post-change, CI coverage per business service)
- Data model standardization (e.g. CI Classes, attributes, relationships aligned to ITIL4)
- Data governance including schema versioning, audit trails, owner-assigned responsibilities, security and access controls