1. ARCHITECTURE OF PROPOSED PRODUCTS

Vendors are required to submit detailed product technical specifications organized as defined in this section. The RFP document is intended to supplement the state's Enterprise Architecture Standards, Best Practices and Principles can be found on the state portal at the address located below.

http://www.ct.gov/best/cwp/view.asp?a=3978&q=462024&bestNav=|

If vendor can supply more than one unique product type, version or level of their software that meets or exceeds the requirements in this RFP, vendor must clearly state the existence of multiple products, explain the major differences between them and take these additional steps:

- Provide separate Product Version and Architecture statements for each.
- Complete a Functional Requirements Vendor Response Form for each.
- Provide clear and separate statements in any proposal sections or sub-sections where there are differences between product versions.
- Provide separate cost schedules and total cost if different.
- Identify which is the vendor's preferred solution and why.

1.1 PRODUCT VERSION

Provide product version information which must include, but not be limited to, product name, version number(s), dates the version was released for general use and the number of installed customer entities (installed base) as of the date you are submitting your proposal.

If product has any Web accessibility, it must comply with the State of Connecticut's "*Universal Web Site Accessibility Policy for State Web Sites - Version 4.0*" and vendors are required to explain how their solution meets this requirement. Information on this policy can be found at http://www.ct.gov/DAS/BEST/cwp/view.asp?a=1306&q=255004

1.2 PRODUCT ARCHITECTURE

Vendor must present a detailed architecture design for the proposed product along with a text description and annotated diagram (or diagrams). Descriptions and diagrams must clearly identify Middleware products, interfaces, message formats and component function. Each description/diagram should be accompanied by a narrative indicating where the proposal meets the State of CT technical guidelines and where exceptions will occur.

1. **Server descriptions**—general functions and operational software components deployed (e.g., IIS, FTP, other services activated).
2. **Network**—servers and the zones (user, DMZ, server zone, database zone at minimum) in which the servers are hosted, firewalls, network protocols, port requirements (specific port, range, configuration capability). This description should include both internal (agency, DAS/BEST, etc.) and external environments (as appropriate).
3. Describe each server to server connection and communications dialog with protocols, type of message or content and paths. The diagrams should also show the (numbered) sequence of the communications dialog. These descriptions should include both internal (Agency, DAS/BEST, etc.) and external environments (as appropriate).

   If your design does not use message-based interfaces between components or systems, you must explain your rationale for such a design. You must explain what the impact would be if you are required to use message-based interfaces between components or systems.
4. The State is now requiring the use of XML as "the" format for most inter-application messaging. You must explain how your proposed design utilizes XML for this purpose. You must explain how your design utilizes XML between components for intra-application messaging. You must identify the source of the XML Schema or Document Type Definitions (DTDs) utilized in your design.
5. The implemented solution must comply with the Department of Administrative Service's Enterprise Architecture (EA) standards, best practices and principles.

2. ARCHITECTURE GUIDELINES FOR WEB BASED APPLICATIONS

2.1 PURPOSE

These Web Development Guidelines are intended to inform prospective bidders of the State's IT architecture, including various standards and guidelines that support our web-based computing environments – Intranet, Extranet, and Internet.

2.2 BACKGROUND

The State has built, and is committed to maintaining a secure, cost effective computing environment capable of supporting various web pages and applications. The State must protect its investment by ensuring that vendors develop according to the State's architecture requirements. Compliance with these standards will ensure the portability necessary to host agency applications and web pages and will also ensure the compatibility, reusability, and scalability of applications. The goal of these standards and architectures is to enhance an agency's ability to shorten development time, ensure security and reliability, and extend application longevity.

In addition to the guidelines within this document, the State has adopted a set of Conceptual Architecture Principles. These principles are intended to align technology solutions that meet the current business needs of the State.

In sum, to make the highest and best use of the State's IT assets, these guidelines have been prepared. Compliance with the standards and guidelines shall be considered when evaluating proposals for state computer systems. The Department of Administrative Services (DAS/BEST) will not approve any procurement for products or services that would result in a contravention of these guidelines.

2.3 REQUEST FOR WAIVER

Deviation from these guidelines requires prior approval by DAS/BEST. The existing Architecture Exception process should be used for this purpose.

2.4 REQUIREMENTS

Web applications shall be designed with the presentation, business logic and data layers both logically and physically separated to increase portability, scalability, re-usability and to support simplicity. This design is commonly referred to as n-tier application development architecture. The State requires the use of at least 3 logical tiers implemented as at least 3 physical security zones. These tiers are presentation, business or application logic, and data base (or data storage).

As an example using a Microsoft based solution architecture this would imply an IIS web server, a separate IIS based application server (for ASP.NET, or VB.NET or C#.NET object and application components, plus data access, and an SQL Server or other DBMS on a third server. These servers are physically located in security zones isolated from one another by firewalls. (Note: VMWare partitions can be used instead of physical servers, but the traffic between the partitions must be through either hardware or software firewalls.)

1. **Technology Standards**. The State maintains a dynamic listing of current technology standards for consideration in new application and web page development. These are available in Section 5 of this appendix or on the DAS/BEST website at the following URL: (http://www.ct.gov/DAS/BEST/cwp/view.asp?a=1245&q=253976&DAS/BESTNav=|

2. **Accessibility**. All applications and pages developed for the State must be compatible with the principles and goals contained in the electronic and information technology accessibility standards adopted by the Architectural and Transportation Barriers Compliance Board under Section 508 of the Federal Rehabilitation Act of 1973 (29 U.S.C. 749d), as amended, and with the State Accessibility guidelines developed pursuant to HEA 1926, Acts of 2001.

   These guidelines are listed via a link available at: http://www.access.state.ct.us/policies/accesspolicy40.html.

3. **Hosting.** Both the logical and physical separation of the presentation, application and database layers is crucial to the State's hosting strategy. The Technical Review Group will conduct a technical evaluation of each application. This evaluation, among other reviews, will determine the appropriate location and security zone for hosting each of the presentation, application and database layers/servers. The technical evaluation will occur in the Business Requirements Analysis phase (or early in the System Design phase) of the State's System Development Methodology.

4. **Support.** Unless exempted in a RFP or an ITB, vendors are required to include a plan for ongoing application and page support. The plan shall include information regarding the appropriate technical skill sets and approximate quantity of support required. The plan shall also identify whether application support is to be conducted from within the State's network backbone or from an external source outside of the State's firewall systems which must be done using the State VPN.

5. **Security – Protocols.** Only HTTP and HTTPS traffic (port 80 and port 443) will be allowed from the client to the Presentation layer through the State's firewall systems for Internet based applications. Extranet applications must use the State VPN for communications between the client and Presentation layer. Applications requiring additional ports opened on the State's firewall systems are strongly discouraged. In all cases, no direct client access to either the Business Logic layer or Database layer will be permitted. If a specific technical solution requires that additional firewall ports be opened, then the presentation of that technical solution must include and clearly identify the advantages to the state for taking on such an additional security risk. Applications and solutions will be designed to allow for the configuration of ports utilized at implementation, however, applications and solutions will not utilize or implement dynamic allocation of ports.

6. **Security - Presentation Layer Input Validation.** Safeguards must be included in all applications to protect the State's data and technical resources. Presentation layer coding must include (at a minimum) specified user input validation checks to guard against unauthorized access. See Enterprise Architecture on the DAS/BEST website and Section 4 of this document regarding Open Web Application Security Project (OWASP) presentation layer input validation guidelines.

7. **Security – Web Authentication.** The State's direction is to allow users to input the same username and password to access different services. This strengthens the State's goal of providing a common look and feel environment in which users perceive they are interacting with State government as a whole, as opposed to many agencies and departments individually. The State has adopted a single sign-on solution utilizing Novell E-Directory, ID Mgr, Access Mgr services. The use of a secondary or alternate sign-on process is not allowed. All agency-specific secondary sign on processes are in addition to, not in lieu of, the above mentioned authentication products. Multiple factor authentication is also allowed as a complement to the single sign-on solution the use of Active Directory for authentication is limited to Exchange, legacy support and file and print scenarios. Agencies should have a complete and uniform vetting process for employee identifications, role establishment and association. A formal set of more complete guidelines has been developed and is available.

8. **Security Review.** The State reserves the right to test all applications from a security perspective and require that any vulnerability identified by such testing be subject to remediation. Testing will occur prior to implementation and may occur post implementation (possibly on a recurring basis).

9. **Documentation.** All system architectures, applications and application components will be documented at a level sufficient to allow for individuals other than the original developer(s) to maintain, support and enhance the application solution. Described in Section 1.2.

10. **Source Code.** The State retains the right to review application source code prior to implementation and while in production status.

11. **Development, Test and Production Servers, Monitoring and Logging.** All web-based applications must be tested in an appropriate n-tiered environment to ensure compatibility, reliability and reasonable performance under load while operating in the State's production environment. It is anticipated that the sophistication and completeness of the testing environment, tools and procedures will be proportional to the size and complexity of the target system. The test environment configuration, tools and procedures will be presented to the agency and the production hosting organizations for review and approval. Applications in development or test status will not be permitted on production servers.

12. **Disaster Backup and Recovery (DBAR).** All critical applications will be designed with Disaster Recovery and Business Continuity in mind. The planning and documentation of such critical applications will include the necessary DBAR content.

3. CONCEPTUAL ARCHITECTURE PRINCIPLES

The state's Enterprise Architecture Standards, Best Practices and Principles can be found on the state portal at: http://www.ct.gov/best/cwp/view.asp?a=3978&q=462024&bestNav=|

3.1 BUSINESS ORIENTED

1. Information is valued as an enterprise asset, which must be shared to enhance and accelerate decision-making.

2. The planning and management of the State's enterprise-wide technical architecture must be unified and have a planned evolution that is governed across the enterprise.

3. Architecture support and review structures shall be used to ensure that the integrity of the architecture is maintained as systems and infrastructure are acquired, developed and enhanced.

4. We should leverage data warehouses to facilitate the sharing of existing information to accelerate and improve decision-making at all levels.

5. IT systems should be implemented in adherence with all security, confidentiality and privacy policies and applicable statutes.

6. The enterprise architecture must reduce integration complexity to the greatest extent possible.

7. Systems must be designed, acquired, developed, or enhanced such that data and processes can be shared and integrated across the enterprise and with our partners.

8. We will consider re-use of existing applications, systems, and infrastructure before investing in new solutions. We will build only those applications or systems that will provide clear business advantages and demonstrable cost savings

9. New information systems will be implemented after business processes have been analyzed, simplified or otherwise redesigned as appropriate.

10. Adopt a total cost of ownership model for applications and technologies which balances the costs of development, support, disaster recovery and retirement against the costs of flexibility, scalability, ease of use and reduction of integration complexity.

11. Create a small number of consistent configurations for deployment across the enterprise.

12. A standardized set of basic information services (e.g., email, voicemail, e-forms) will be provided to all employees.

3.2 TECHNOLOGY ORIENTED

1. Applications, systems and infrastructure will employ reusable components across the enterprise, using an n-tier model.

2. The logical design of application systems and databases should be highly partitioned. These partitions must have logical boundaries established and the logical boundaries must not be violated.

3. The interfaces between separate application systems must be message-based; this applies to both internal and external systems.

4. We must deploy application systems that are driven by business events.

5. We should separate on-line transaction processing (OLTP) from data warehouse and other end-user computing.

6. The State shall adopt and employ consistent software engineering practices and methods based on accepted industry standards.

3.3 BUSINESS CONTINUITY ORIENTED

1. IT solutions will use industry-proven, mainstream technologies.

2. Priority will be given to products adhering to industry standards and open architecture.

3. An assessment of business recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing systems. Based on that assessment, appropriate disaster recovery and business continuity planning, design and testing will take place.

4. We must implement a statewide backbone network that provides a virtual, enterprise-wide local area network

5. The underlying technology infrastructure and applications must be scalable in size, capacity, and functionality to meet changing business and technical requirements.

5. DAS/BEST STRATEGIC STANDARDS AND PRODUCTS

Information technology applications will be required to follow the Enterprise Architecture standards described in this section and in the tables below. Version levels represent the minimum accepted level.

The state's Enterprise Architecture Standards, Best Practices and Principles can be found on the state portal at: http://www.ct.gov/best/cwp/view.asp?a=3978&q=462024&bestNav=|

5.1 REQUEST FOR WAIVER

Deviation from these guidelines requires prior approval by DAS/BEST. The existing Architecture Exception process should be used for this purpose.

5.2 QUESTIONS

Any questions related to the material presented in this document or on the state's Enterprise Architecture portal are encouraged and are expected to comply with the procedures for addressing questions, as outlined in the main RFP document.