

**Florida Drug Court Case Management System (FDCCMS) ITN #10-001AG
Questions and Answers**

- 1. Q: We believe there is an inconsistency in the ITN document page 12, numeral 6.5.9 Ownership of Software, paragraph (1). After reading it seems that OSCA is purchasing something that already owned. Is that right?**

A: No. The OSCA is interested in purchasing new software.
- 2. Q: Given the above: Are you looking for an already built commercial package modified to meet your needs? Or, for a customized tailored application?**

A: Either type of application will be considered if it meets the OSCA's needs.
- 3. Q: If you are looking for a customized solution and given the restrictions to learned firsthand from court personnel (page 22, numeral 7.3), why do you ask for detailed functional software description? (page 23, num 7.8 paragraph 1 - Fully Describe the Software Application)**

A: The restriction listed on page 22, 7.3, is strictly related to the ITN. Any questions regarding the ITN and any requirements listed therein, should have been included in your list of submitted questions. Regarding page 23, 7.8, regardless of whether your proposed solution is a Commercial Off The Shelf (COTS) package, a COTS plus custom coding or a fully custom coded solution, you should be able to provide a functional description of your proposed solution that will be based on the requirements outlined in the ITN.
- 4. Q: Given the idea to have customized software, what is the reason for assigning 20 points towards a design not yet created?**

A: The ITN does not assign 20 points to a design that has not yet been created.
- 5. Q: Regarding the evaluation criteria, experience. How many points an expert in the IT and software solutions, with proven alternate experience in other areas, will get out of those 25 points?**

A: All proposals will be based on the criteria set forth in the ITN.
- 6. Q: Does OSCA already have an approved fuzzy logic search software? If yes, can you identify the approved software? If no, is it within the scope of this ITN to propose an alternative fuzzy logic search software?**

A: The OSCA is testing fuzzy logic search software but has not procured any particular software. The intent of putting this in the ITN was to make the vendor aware that there will be some requirement to utilize such software. And, as specified on page 18, 6.10, the OSCA will review any proposed software and make a determination at that time if such software is compatible and supportable within our environment.

7. **Q: Will a solution be precluded from consideration if it proposes a solution that includes other than the named fuzzy search software already approved by OSCA?**

A: The OSCA is testing fuzzy logic search software but has not procured any particular software. The intent of putting this in the ITN was to make the vendor aware that there will be some requirement to utilize such software. And, as specified on page 18, 6.10, the OSCA will review any proposed software and make a determination at that time if such software is compatible and supportable within our environment.

8. **Q: In section 6.11, there are court Standards and Specifications, as required can you please provide us with copies of all your standards and specifications? In addition can you please provide documentation for:**

- a. Current OSCA Court Technology Standards**
- b. ISS Change/production management and change control procedures. (Section 6.5.1)**
- c. ISS application security requirements and standard. (Section 6.5.1 and 6.5.8)**
- d. Operational requirements and standards for backup and disaster recovery established by ISS mentioned in 6.5.10**

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the attached application and database standards.

9. **Q: It appears that we will be augmenting existing operational drug and/or existing court case management systems throughout the State of Florida to capture and manage relevant drug court data to generate reports that will allow the State to better monitor the success/failure of drug courts. Can you please confirm?**

A: The OSCA is looking for a new statewide case management system to supplant any existing drug court case management system being utilized by local drug court programs.

10. **Q: Section 7.8 specifies the proposal outline and the maximum page count for sub-sections that total 33 pages. In Section 9, additional proposal requirements are added including the Executive Summary, Staff Qualifications, Technical and Functional Certification documentation, Financial Information, Federal Requirements, and References. However, in Section 8, it states that "proposals shall be limited to 25 PAGES in length.." Can you please clarify your expectation regarding maximum proposal length?**

A: All proposals shall be limited to a total maximum of 33 pages in length according to section 7.8 of the ITN. Section 8.0 erroneously indicates a limit of 25 pages.

11. **Q: In Section 6.12.3 Project Schedule, there is a date entered under Project Closeout of 9/30/2011. Does this indicate that the OSCA requires that the project be completed by this date?**

A: Yes.

12. **Q:** "The response instructions for the Invitation to Negotiate do not ask for Vendor pricing. However, Section 7.7 states that "A Vendor shall not collude, consult, communicate, or agree with any other Vendor regarding this ITN as to any matter relating to the Vendor's cost proposal". In addition, in Section 10.0 "Evaluation Criteria" element "c" it states "Costs as indicated in cost projection sheets in relation to the functionality provided" is worth 20 points. There is no cost projection sheets provided nor any requirements associated to pricing within the ITN. Can you confirm that a cost proposal is not required as part of the Vendor response and if it is, can you please provide additional direction as to the Cost Proposal requirements.
- A:** A cost proposal is required. The vendor should use the phases table in section 6.12.1 of the ITN. The vendor should breakdown cost by applicable phases with a total cost included. The document should be provided as a separate attachment and is not part of the 33 page maximum length requirement for the proposal.
13. **Q:** Please clarify the difference between the two client references requested in the Executive Summary and the three references requested in Section 9.6. Are a total of 5 separate references required?
- A:** All proposals shall require a total of 3 separate references, two of which should include documented experience in the criminal justice and drug court area.
14. **Q:** Can you please provide the relevant documentation regarding standards and specifications provided in the table in Section 6.11
- A:** The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards.
15. **Q:** In 6.5.7 there is a reference to data conversion however there is little information as to the specifications and scope. Could you please provide further information?
- A:** The current drug court expansion project application is in .Net 3.5 and SQL Server 2005. The database currently tracks approximately 700 clients but is constantly increasing. The data contained in this database will need to be converted and included as historical information in the new solution. There may also be data from specific Circuit/County drug court applications that will need to be converted into the new solution as well.
16. **Q:** How many external systems will we be integrating with and will we have access to the technical specifications prior to the submittal due date?
- A:** The system will only be intergrading with JIS initially. All data sources listed on page 9, 6.3.13, are accessible via JIS. FCIC certification is required to access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The system should allow for future

integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

17. Q: Can you provide details about the envisioned functionality when interfacing with JIS including data elements that will be involved and the technical details of the JIS application interface mentioned in 5.1.2 and 6.3.13?

A: The system will only be intergrading with JIS initially. At least these functionalities: 1. Capability to access JIS search interface for the purpose of having the case manager search for the appropriate drug court client and return any needed person information to be recorded in the drug court database. 2. Web service(s) to get/accept event data from JIS such as an arrest has occurred. Data elements for either would include the following: Person/client information, arrest information, and other event information, as determined by the OSCA. FCIC certification is required to access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

18. Q: 6.3.5 mentions other state databases to be matched. Can you provide details about those state databases including their data formats and data elements?

A: The system will only be intergrading with JIS initially. All data sources listed on page 9, 6.3.13, are accessible via JIS. FCIC certification is required to access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

19. Q: 6.3.6 mentions interfacing with other internal and external data stores. Can you provide information on the number of different stores, their formats, data that they contain and their interfacing capabilities/requirements?

A: The system will only be intergrading with JIS initially. All data sources listed on page 9, 6.3.13, are accessible via JIS. At least these functionalities: 1. Capability to access JIS search interface for the purpose of having the case manager search for the appropriate drug court client and return any needed person information to be recorded in the drug court database. 2. Web service(s) to get/accept event data from JIS such as an arrest has occurred. Data elements for either would include the following: Person/client information, arrest information, and other event information, as determined by the OSCA. FCIC certification is required to access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

20. Q: 6.3.12 mentions interfacing with existing State of Florida data systems. Can you provide information about those Systems their formats, data that they contain and their interfacing capabilities/requirements?

A: The system will only be intergrading with JIS initially. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

21. Q: **Can provide more information regarding the intended functionality of the OSCA approved fuzzy logic search software to be interfaced with? Is the intent to do searches on the data captured in the drug court database? We assume OSCA will provide this SW.**

A: The intent of the fuzzy logic search software is to conduct drug court participant matches from the drug court case management system to those individuals in JIS. The OSCA will be providing this software.

22. Q: **Will OSCA/ISS procure System SW and HW directly for this solution or will the Vendors be asked to provide those?**

A: Per page 18, 6.10, if the solution is to run in the Courts environment, the OSCA will utilize our own hardware, software and licenses for production unless approval is granted in writing. For instance, if the solution is a hosted solution, the vendor hosting the solution would be responsible for the licenses, hardware and software for production.

23. Q: **Page 6 states, "The data elements to be included in the state-wide system are not limited to the list located in Attachment D. {This list illustrates some of the fundamental data elements necessary to support daily drug court operations and statewide drug court evaluation(s).}" Can you provide any additional elements that are not included in Attachment D? Can you provide an estimate of how many additional elements may be included in the system (outside of those listed in Attachment D)?**

A: A comprehensive list of additional data elements is not available at this time.

24. Q: **Item 11 of section 6.5.5 states that SQL Server Integration Services is to be used for jobs. Please provide examples of possible jobs. Would you accept other methods/tools for batch processing and integration jobs along with SQL Server Integration Services? Or Is SQL Server Integration Services required for job processing?**

A: Because our supported technical environment is a Microsoft environment, the OSCA requires the use of certain software that the OSCA already has provided at the enterprise level. For automated jobs, the OSCA requires the use of SQL Server Integration Services.

25. Q: **Perficiant is the USA distributor for a State Government Case Management System called GoPro. Generally speaking GoPro looks like a fit for this application. GoPro has been built using IBM Technologies including Java, FileNet for Electronic Content management and WebSphere Portal for viewing the information. Section 6.5.1 requires Microsoft C# and .Net as the development platform. GoPro uses IBM Java as the development platform. Does the use of Java as the development platform eliminate GoPro as a potential solution?**

A: Given the provided description of GoPro, it would not be considered as a solution because it does not meet the requirements of section 6.5. Specifically, the OSCA does not support Java, FileNet or WebSphere Portal in the OSCA technical environment.

26. **Q: You have given high level functional level requirements in section 6.3 and other places. Can you provide us detailed functional specifications? Examples: Screens, Data fields on screens, calculations behind the scenes, report formats, relationship between data elements, functional flow charts, number & types of users, capabilities associated with each type of users,**

A: No. Detailed functional specifications are not available at this time. Refer to sections 6.2 and 6.3 of the ITN.

27. **Q: You mentioned that you want interfaces with other systems such as JIS but no specific details were given. Can you specify details please?**

A: The system will only be intergrading with JIS initially. All data sources listed on page 9, 6.3.13, are accessible via JIS. At least these functionalities: 1. Capability to access JIS search interface for the purpose of having the case manager search for the appropriate drug court client and return any needed person information to be recorded in the drug court database. 2. Web service(s) to get/accept event data from JIS such as an arrest has occurred. Data elements for either would include the following: Person/client information, arrest information, and other event information, as determined by the OSCA. FCIC certification is required to access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

28. **Q: Do you have a preference between COTS package and Custom Development Software where the vendor will come to your offices take requirements/functional charts and develop as per specifications?**

A: Either type of application will be considered if it meets the OSCA's needs.

29. **Q: If the vendor does not have specific experience in Drug court cases but has experience with general court case management then would they be at a disadvantage (with respect to references and section 10 item (a) of Evaluation Criteria?**

A: According to section 9.1 of the ITN, vendors without documented experience in the criminal justice and drug court areas will be affected in the evaluation outlined in section 10.0 of the ITN.

30. **Q: How many JFA instances will we be expected to interface/integrate with? JIS would be a centralized system but JFA is county by county**

A: If this question pertains to JLA, there would be a need to interface with each JLA county calendar (approximately 50 counties.) This is via JIS.

31. **Q: Would our solution be expected to interface with AWAC? If so, how many instances of AWAC would we connect to?**

A: No.

32. **Q: How will these systems (case management) interface? Web services, Staging tables, etc?**

A: The OSCA envisions a combination of both web service(s) and staging tables. Per page 6, 5.2, modifications to the JIS Java code are not included in the scope of this project. However, per page 6, 5.1, system interface code to access JIS is part of the scope of this project.

33. **Q: Is use of .net architecture required for COTS solution components?**

A: Yes. Because our supported technical environment is a Microsoft environment, the OSCA requires the use of certain software that the OSCA already has provided at the enterprise level. These architecture requirements are specified on page 9, 6.5.

34. **Q: 6.3.10 Which data analysis tools will be used/required? Is that the use of SQL Server Reporting Services (noted in other sections) or will extensive data analysis tools within the system be required? (And if so, please IDENTIFY)**

A: The OSCA has SQL Server Analysis Services available in the enterprise environment. This would be appropriate to use for any data analysis, statistical analysis and multi-dimensional data analysis. SQL Server Reporting Services would be used for reporting. However, as stated on page 18, 6.10, the OSCA will consider and make a decision on any other data analysis software proposed by the vendor.

35. **Q: 6.3.12 interface to other state systems...**

- Which systems?
- How many?
- What will be the interface methodology of those systems?
- Is the question "can your system interface with other systems beyond this rfp"?
- Are those systems to be included in this initial rfp response / scope?

A: The system will only be intergrading with JIS initially. All data sources listed on page 9, 6.3.13, are accessible via JIS. At least these functionalities: 1. Capability to access JIS search interface for the purpose of having the case manager search for the appropriate drug court client and return any needed person information to be recorded in the drug court database. 2. Web service(s) to get/accept event data from JIS such as an arrest has occurred. Data elements for either would include the following: Person/client information, arrest information and other event information, as determined by the OSCA. FCIC certification is required to access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The OSCA envisions a combination of both web service(s) and staging tables. Per page 6, 5.2, modifications to the JIS Java code are not included in the scope of this project. However, per page 6, 5.1, system interface code to access JIS is part of the scope of this project. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

36. **Q: Will the 50 adult drug courts have their own case management systems from which this solution will extract information? If so;**

- How many DRUG COURT CASE MANAGEMENT systems will our solution be expected to interface/integrate with?

- **Will the Drug Court Case Mgmt System be required to provide real-time updates to other systems (District Atty, other courts)?**

A: The OSCA is looking for a new statewide case management system to supplant any existing drug court case management system being utilized by local drug court programs.

37. Q: 6.3.14/ 6.5.6 What “fuzzy logic” software and data stores are we expected to interface with?

- **Type of interface? What are the “Info to be shared” rules, etc?**

A: The OSCA is testing fuzzy logic search software but has not procured any particular software. The intent of putting this in the ITN was to make the vendor aware that there will be some requirement to utilize such software. And, as specified on page 18, 6.10, the OSCA will review any proposed software and make a determination at that time if such software is compatible and supportable within our environment. The OSCA does not know what is meant by "info to be shared" rules, etc.

38. Q: 6.5.1 Follow ISS established ... How can the respondent obtain these procedures or will these procedures be provided before the response is due?

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards.

39. Q: 6.5.3 (1) Use C# .Net as the language for .Net development. If the product is a COTS product and will remain a COTS product even with modifications to software to meet OSCA requirements for this ITN is C# required?

A: Because our supported technical environment is a Microsoft environment, the OSCA requires the use of certain software that the OSCA already has provided at the enterprise level. These architecture requirements are specified on page 9, 6.5. .Net is required. The OSCA will consider COTS solutions that are coded in vb.Net.

40. Q: 6.5.7 Data conversion requirement

- **How many systems own the data to be converted?**
- **Where does that data reside now?**
- **In what format does that data reside?**
- **What is volume of that data?**

A: The current drug court expansion project application is in .Net 3.5 and SQL Server 2005. The database currently tracks approximately 700 clients but is constantly increasing. The data contained in this database will need to be converted and included as historical information in the new solution. There may also be data from specific Circuit/County drug court applications that will need to be converted into the new solution as well.

41. **Q: 6.5.10 How can the respondent obtain these procedures?**
- **Will they be provided before the response is due?**
 - **Is the respondent expected to develop and/or incorporate Backup, Business Continuity, Disaster Recovery?**

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards. As listed on page 19, one of the deliverables is a Disaster Recovery Plan. This plan must work with the deliverable, Operations and Support Plan also. Per page 12, 6.5.10, the vendor's solution shall conform to backup and operational requirements/standards that OSCA has established. Per page 13, 6.5.10, the vendor must conduct an actual application recovery using the Disaster Recovery Plan/Manual prior to it being accepted as a deliverable. This recovery exercise will be conducted with OSCA staff.

42. **Q: 6.0 Can OSCA provide standards and guidelines document prior to responses being due to insure vendor is aware of all standards and guidelines?**

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards.

43. **Q: 6.6 (3) How can the respondent obtain the procedures and templates?**

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards.

44. **Q: 6.6.2 (1) How can the respondent obtain the OSCA approved Project Management procedures and templates?**

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards. Per page 13, 6.6, all

documentation shall meet or exceed the minimum requirements of the Project Deliverables Matrix, provided in the ITN. Per page 14, 6.6.3, the vendor has the option to use their own Project Management protocol and templates as long as OSCA approves their use of it.

45. Q: 6.6.3 How can the respondent obtain the ISS Project Management procedures and templates or an approved internal Project Management protocol?

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards. Per page 13, 6.6, all documentation shall meet or exceed the minimum requirements of the Project Deliverables Matrix, provided in the ITN. Per page 14, 6.6.3, the vendor has the option to use their own Project Management protocol and templates as long as OSCA approves their use of it.

46. Q: 6.7.3 (b)(xi) Roll-Out

- **Is equipment part of this ITN or an option?**
- **Will the state provide (server) hardware?**
- **How many locations are identified for roll-out?**
- **How are they located geographically?**
- **Is it expected that roll-out will require vendor on-site at each roll-out location for some period of time?**

A: Per page 18, 6.10, if the solution is to run in the Courts environment, the OSCA will utilize our own hardware, software and licenses for production unless approval is granted in writing. For instance, if the solution is a hosted solution, the vendor hosting the solution would be responsible for the licenses, hardware and software for production. The database and web application portion of the solution would be consolidated and centralized in Tallahassee.

47. Q: 6.8 Training:

- **Will use of Camtasia (recording training) suffice for the “computer based training” requirement? It seems people could watch that and use the “training” data on their system to go through the training as needed.**

A: Yes.

48. Q: 6.8.2

- **Will a webinar suffice for enhancing (not replacing) lab based Train the Trainer sessions?**
- **Approximately, how many users should the respondent propose?**

A: If all training requirements are met as stated in the ITN, any training tools enhancing lab based training will be considered. Approximately 100-200 users will require training.

49. Q: 6.8.3

- **Approximately, how many OSCA staff should the respondent propose?**

A: Approximately 20 OSCA staff will require training. This includes technical knowledge transfer for supporting the platform and understanding operational requirements.

50. Q: 6.11 –

- **The ITMN states that “vendors who need a copy of any documents referenced herein should submit a request to the contact on page 24”**
- **THERE IS NO CONTACTS ON PAGE 24.**
- **Should we use the contacts on page 22 to request ISS and OSCA procedures and templates?**
- **Should we contact Mr. Gerson or Mr. Long?**

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards. Contact Aaron Gerson as specified in section 7.2 page 22 of the ITN.

51. Q: 6.12.1-

- **Is a proposed MS-Project plan, outlining the deliverables, to be provided as part of the response to this ITN?**

A: Yes.

52. Q: 6.12.3 –

- **Is the respondent expected to provide the Due Dates, based on a proposed project plan, as part of the response?**

A: Yes.

53. Q: 7.1 Time Line – Which is CORRECT? · Page 22 paragraph 7.0 The deadline date and time for receipt of proposals is 12/13/10 at 3:00pm · Page 25, 8.0 second paragraph – the deadline is 12/13/10 at 5:00pm. · Which is the correct time?

A: The correct deadline is 12/13/10 at 3:00 p.m. EST as stated in section 7.1 page 22 of the ITN. Section 8.0 erroneously indicates 5:00 p.m.

54. Q: 7.8 (6) –

- **Is the State requesting a sample of technical documentation, user and training manuals be provided as part of the response or simply a description there of?**

A: A description of documentation is required. It is optional to provide samples of documentation. Samples of documentation must be provided in a separate file and will not be considered as part of the 33 page maximum length requirement for the proposal.

55. Q: 9.3 –

- Will OSCA provide current court technology standards?

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards.

56. Q: 12.0 – Addendum –

- Will OSCA and ISS processes, procedures, templates, and documents, referenced within this ITN be posted at www.flcourts.org/gen_public/purchasing?

A: No other documents other than what is posted at www.flcourts.org will be provided.

57. Q: 13.1.12 -

- This paragraph states that the response is binding to the vendor for 60 days after opening.
- Page 25, 8.0. states: “The response is binding to the vendor for 30 days after opening”.
- Which is correct?

A: The correct response is binding to the vendor for 60 days according to section 13.1 section 12 of the ITN. Section 8.0 erroneously indicates 30 days.

58. Q: PRICING:

- In what format does OSCA want the respondent’s PRICING PROPOSAL?
- Should pricing be proposed as a separate document and not as part of the Technical/Business Response?
- Should pricing be provided in the Financial Section of the response?

A: A cost proposal is required. The vendor should use the phases table in section 6.12.1 of the ITN. The vendor should breakdown cost by applicable phases with a total cost included. The document should be provided as a separate attachment and is not part of the 33 page maximum length requirement for the proposal.

59. Q: Is there a proposed budget for the project? If so what is the amount?

A: Yes. However, the amount will not be provided at this time.

60. Q: What is the anticipated annual case volume once system is deployed?

A: Approximately 11,000 cases annually with the ability to expand.

61. Q: Is the data required for the conversion resident in one or multiple systems? If multiple systems, please state number of systems and what data format(s)?

A: The current drug court expansion project application is in .Net 3.5 and SQL Server 2005. The database currently tracks approximately 700 clients but is constantly increasing. The data contained in this database will need to be converted and included as historical information in the new solution. There may also be data from specific Circuit/County drug court applications that will need to be converted into the new solution as well.

62. Q: In Section 7.8 of the ITN it states that "A Vendor's proposal must be submitted as outlined below", and lists off items 1-7 each of which state a certain page count that totals to 33 pages. But then in Section 8.0 (Proposal Preparation) it states "Proposals shall be limited to 25 pages in length, unless prior approval has been obtained from the OSCA to extend the document length. Proposals will not be evaluated on length but rather clarity and depth". Is Section 7.8 considered OSCA's approval to extend the document length, and if so are we to also include the items requested in Section 9.0 (Proposal Requirements) and are these also limited to these page counts?

A: The proposals shall be limited to a total maximum of 33 pages in length according to section 7.8 of the ITN. Section 8.0 erroneously indicates a limit of 25 pages.

63. Q: Architecture: If we propose a COTS solution, is it required to be based on a .NET platform? Would you consider a web-based system developed in JAVA that would run with a SQL server database?

A: Because our supported technical environment is a Microsoft environment, the OSCA requires the use of certain software that the OSCA already has provided at the enterprise level. These architecture requirements are specified on page 9, 6.5. .Net is required.

64. Q: Users: How many users will be utilizing the analytics/reporting tools?

A: Refer to section 6.5.4 subsection 4 of the ITN.

65. Q: Interfaces: The ITN indicates the requirement to interface with other electronic data stores in addition to JIS. For the other electronic data stores, please provide the following:

- Anticipated number of additional interfaces
- For each anticipated additional interface, please provide the name of the application to connect with, the development platform of the application, the database type of the application, the type of interface (one-way receiving of information into the CMS, one-way sending of information to the CMS, bi-directional), and the data elements to be transferred (indicating source and receiving system for each data element)

A: The system will only be intergrading with JIS initially. All data sources listed on page 9, 6.3.13, are accessible via JIS. At least these functionalities: 1. Capability to access JIS search interface for the purpose of having the case manager search for the appropriate drug court client and return any needed person information to be recorded in the drug court database. 2. Web service(s) to get/accept event data from JIS such as an arrest has occurred. Data elements for either would include the following: Person/client information, arrest information and other event information, as determined by the OSCA. FCIC certification is required to

access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The OSCA envisions a combination of both web service(s) and staging tables. Per page 6, 5.2, modifications to the JIS Java code are not included in the scope of this project. However, per page 6, 5.1, system interface code to access JIS is part of the scope of this project. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

66. Q: Interfaces: For interfaces, the ITN indicates a desired interface with “fuzzy logic search software.” Please provide the name or names of the potential search software and also the types of data to be available to be searched.

A: The system will only be intergrading with JIS initially. All data sources listed on page 9, 6.3.13, are accessible via JIS. At least these functionalities: 1.Capability to access JIS search interface for the purpose of having the case manager search for the appropriate drug court client and return any needed person information to be recorded in the drug court database. 2. Web service(s) to get/accept event data from JIS such as an arrest has occurred. Data elements for either would include the following: Person/client information, arrest information and other event information, as determined by the OSCA. FCIC certification is required to access JIS (no exceptions), that also includes developers, systems analysts, software architects, project managers, etc. There is no cost for the training, certification or fingerprinting. The OSCA envisions a combination of both web service(s) and staging tables. Per page 6, 5.2, modifications to the JIS Java code are not included in the scope of this project. However, per page 6, 5.1, system interface code to access JIS is part of the scope of this project. The system should allow for future integration with other systems such as those operated by treatment providers, state attorney's offices, and others.

67. Q: Conversion: For conversion of Drug Court Expansion Program data, is the data from all state drug courts in one central system or repository today, or is this data in 50 different drug-court level systems?

A: The current drug court expansion project application is in .Net 3.5 and SQL Server 2005. The database currently tracks approximately 700 clients but is constantly increasing. The data contained in this database will need to be converted and included as historical information in the new solution. There may also be data from specific Circuit/County drug court applications that will need to be converted into the new solution as well.

68. Q: Conversion: For conversion of Drug Court Expansion Program data, please provide the following:

- **Name and number of Drug Court Expansion Program system(s)**
- **Platform of Drug Court Expansion Program system(s)**
- **Database of Drug Court Expansion Program system(s)**
- **Types of data to be converted (field names)**
- **Number of records to be converted by system(s)**

A: The current drug court expansion project application is in .Net 3.5 and SQL Server 2005. The database currently tracks approximately 700 clients but is constantly increasing. The data contained in this database will need to be converted and included as historical information in

the new solution. There may also be data from specific Circuit/County drug court applications that will need to be converted into the new solution as well.

69. Q: Training: The ITN request 5 “Train the Trainer” Sessions to include approximately 100 people. Does this mean that 100 people will participate in each of the 5 sessions (500 people total) or that 100 people will be divided between 5 sessions (100 people total, approx 20 people per session)?

A: Approximately 20 people per session for a total of 100.

70. Q: Help Desk: Does the Court or the State of Florida have a help desk available that may support a COTS or custom developed application for initial user (Level 1) help questions?

A: First level support would be in OSCA or via a service agreement with the vendor who will be supporting the application.

71. Q: Timing: The ITN indicates the project closeout date of 9/30/11. Is this date set in stone? Is the closeout date driven by grant funding? Is there an opportunity to extend the close out date?

A: Yes. The closeout date is driven by grant funds. An opportunity to extend the close out date is undetermined at this time.

72. Q: Go-Live: Does the Court intend for all users to begin using the system on the same go-live date, or does the court desire a staggered go-live approach?

A: This should be part of the vendors' proposal project plan based on the strategy for deployment of their proposed solution. The OSCA sees advantages to both. The vendor should outline their proposed method in their proposal.

73. Q: Go-Live: What is the desired go-live date (if rolled-out at one time to all courts) or dates (if roll-out is staggered)?

A: This should be part of the vendors' proposal project plan based on the strategy for deployment of their proposed solution. The solution should be fully implemented by 9/30/2011.

74. Q: Proposal Preparation. Please provide clarification regarding the proposal structure and length. The requirements in section 7.8 total a maximum of 33 pages. In section 9, the proposal is limited to 25 pages and includes additional sections that were not mentioned in section 7.8. Please clarify how many pages the proposal may total, and if additional appendices will be considered to provide additional supporting documentation. Additionally, please provide a summary of the proposal response structure, integrating all desired sections/elements listed in sections 7.8 and 9.

A: The proposals shall be limited to a total maximum of 33 pages in length according to section 7.8 of the ITN. Section 8.0 erroneously indicates a limit of 25 pages. Proposal preparation and requirements are indicated in section 7.8, 8.0, and 9.0 of the ITN.

75. **Q: Functional Requirements: Section 6.3.2 states “Collect data to ensure critical performance indicators can be reported.” Please provide a list of the critical performance indicators to be reported.**

A: Refer to the following link.

http://www.flcourts.org/gen_public/family/drug_court/bin/CriticalPerformance.pdf

76. **Q: Project cost: Will the Court accept a deliverables-based pricing structure? What is the desired format for cost? The ITN references a cost projection sheets in section 10.0 (page 27), but we were unable to locate these in the ITN document.**

A: A cost proposal is required. The vendor should use the phases table in section 6.12.1 of the ITN. The vendor should breakdown cost by applicable phases with a total cost included. The document should be provided as a separate attachment and is not part of the 33 page maximum length requirement for the proposal.

77. **Q: Contractual Terms: Will the Court consider modifications to the contractual language included in the ITN during the contract negotiation process? Or, would the Court prefer that the response include proposed changes to the language of the contract contained in the ITN?**

A: The proposal may indicate any proposed changes to contract language for consideration.

78. **Q: Additionally, per section 6.11 of the ITN, we would like to request an electronic copy of the following standards:**

- **Project Procedures:**
 - Risk and Issue management procedures
 - Quality management procedures
 - Scope change management procedures
- **Architecture standards mentioned in the ITN per section 6.5.1**
 - Information Systems Services (ISS) established change/production management procedures.
 - ISS established change control procedures (if different from above)
 - Database audit trail requirements
 - Application security requirements
- **Technical standards documentation:**
 - Change Management Procedures

A: The OSCA follows the ITIL standard for production Change and Release Management which includes a Change Request submitted via our internal SharePoint site. The OSCA follows industry standards for security, backup and disaster recovery. The OSCA utilizes project management and information systems development methodology (ISDM) templates and procedures based on PMBOK. Templates, internal policies, and procedures will be provided to the chosen vendor, including project management, ISDM, security, backup, and disaster recovery. See the provided application and database standards.

79. **Q: Would you consider a hosted technical solution for the FDCCMS (ITN #10-001 AG)?**

A: Yes.

Florida State Courts Application Security Standards

- ✓ Rely on tested and proven security systems rather than a home grown solution. Use industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.
- ✓ Application should have security provision to implement required authorization level to users on a case by case basis and easily configurable. Role based authorization shall be utilized. The authentication mechanism shall be implemented by Microsoft Active Directory and should be independent of the application and should be easily configurable.
- ✓ Application should validate user inputs for minimum length, maximum length, data type, and special characters. Special characters especially single quote should be allowed only if necessary.
- ✓ Password policy should be maintained in accordance with the Florida State Courts password policy.
- ✓ No sensitive information like user id or password should be stored in computer memory, files, database, or registry (in Windows) in ASCII format. If required, it can be stored in one way hash format (to be decided by Tech Lead / Project Manager).
- ✓ Critical files should be protected by rights and proper access control lists must be maintained.
- ✓ Application should log transactions at all layers. Logging at each layer should be easily configurable and the configuration mechanism should not be embedded in the application code.
- ✓ Application should flush all data stored in memory immediately after its use.
- ✓ Application should not allow passwords to the presentation layer. All required checks for sensitive information must be done at the server/database layer.
- ✓ Application should be able to identify and maintain sessions. Each session ids must be randomly generated by the application.
- ✓ Expose only the functionality that is expected to be used by others.
- ✓ Application should handle errors at each layer and should be converted into a user readable language while displaying on the presentation tier. No sensitive security information (including the component name) should be presented on the User Interface.
- ✓ Default to a secure mode. Don't enable services, account rights, and technologies that are not explicitly needed. While deploying the application on client and/or server computers, its default configuration should be secure.
- ✓ Follow STRIDE principles — STRIDE stands for Spoofing, Tampering, Repudiability, Information disclosure, Denial of service, and Elevation of privileges. (See included Secure Coding Principles document.)

- ✓ Network traffic to and from application server, database server should be protected to maintain confidentiality and integrity.

Reference:

<http://www.webappsec.org>

<http://www.networkworld.com/>

<http://www.owasp.org>

[http://msdn.microsoft.com/en-us/library/eky0e816\(v=VS.90\).aspx](http://msdn.microsoft.com/en-us/library/eky0e816(v=VS.90).aspx)

[http://msdn.microsoft.com/en-us/library/eky0e816\(v=VS.100\).aspx](http://msdn.microsoft.com/en-us/library/eky0e816(v=VS.100).aspx)

<http://msdn.microsoft.com/en-us/library/zdh19h94.aspx>

Secure Coding Principals

An Overview on Secure Coding Principles

Secure coding is the topic of lectures, books, seminars, academic classes and even entire careers. Numerous articles, books, and websites are dedicated to helping programmers understand secure coding. This document is intended as a means to help experienced and novice programmers develop secure code. Good programmers write good code, bad programmers write bad code, but all programmers seem to write insecure code. This is because it is hard to write good secure code. Many programmers don't understand security as it relates to coding. Their main focus in software development is to make it work. Often they have no knowledge or regard for the principles of design, persistence, and exploitation avoidance of secure coding. This poses a problem for everyone who relies on the software they develop, and puts huge liability on the organization from which the code originated. Insecure code can allow an intruder to view sensitive information, change or delete valuable or important data, or to run programs or plant malicious code within the software system they have exploited. For these reasons, security must be a priority for every software developer and programmer.

Security in Design

Secure systems are built by employing the principles of secure coding into the design process and persistently evaluating the security of the application throughout the development process. Many security vulnerabilities could easily be prevented if security were taken into consideration at the beginning of the development process. While it is nearly impossible to come up with a list of every possible vulnerability that could exist as a result of coding oversights, it is possible to understand some of the more typical and common problems that often exhibit themselves as coding weaknesses and vulnerabilities. Some of the most common security exploits are:

- Weak file and group permissions
- Race conditions
- Problems with temporary files and session variables
- Buffer overflows and memory pointer exploits
- Overly complex and unnecessary code
- Hard-coding passwords
- User Input

Knowing these will help protect your applications from the most obvious security issues. Designing and implementing countermeasures to these most common exploits is a good place to start in developing secure applications. Also, enforcing programming standards and persistent regression testing will confirm that the application is secure.

Principle of Least Privilege

Program design should follow the principle of least privilege. This requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. This prevents the disclosure of sensitive data, and prevents unauthorized users from gaining access to programs or areas where they were never meant to be.

Principle of Exclusive Rights

Race conditions occur when the outcome of interrelated events depend on a particular event ordering sequence that cannot be guaranteed making the final state of the system unpredictable. A typical example of this would be if commands to read and write to a particular file are received at the same time. This could result in the overwriting of data before it has been read, the return of incorrect data because it was read prior to writing the updated information, or worse yet, an operating system crash. Utilizing file locking mechanisms and asynchronous responses to called programs can prevent these race conditions from occurring.

Another specific type of race condition called "time of check to time of use" (TOCTTOU) can be created when using temporary files, or session variables. If the temporary file or session variable does not have secure permissions, it could be altered between the time it is created and the time the program later reads from it or writes to it again creating opportunities for exploitation.

The application must have exclusive rights to any files and data for which it relies on for information. Alterations

Secure Coding Principals

and concurrent access cause unexpected program execution and vulnerabilities in security.

Principle of Secure Memory Management

Buffer overflows occur when arbitrary code is injected into assigned application buffer spaces causing unwanted executions of applications or malicious code. Buffer overflows can be prevented by making sure that bounds-checking are done on the length of input variables, arrays, and arguments.

Memory pointers can also be used to execute malicious code or programs. Because memory pointers can be pointed at any memory structure or location, they enforce no ownership of memory and therefore can end up pointing at anything. It's common in attacks on the Windows OS to put malicious code at an address that a pointer references because the OS cannot tell that the code there is foreign. Minimizing the use of memory pointers and destroying them after they are done being used will help to reduce this security threat.

Buffer overflows and memory pointer exploits are of the most common system exploits, as well as the most dangerous. Not only can these exploits cause an application to act unexpectedly, but they can also compromise the security of the entire computer the application is run on, and possibly an entire network if the PC is connected to an unsecured LAN.

Principle of Simplicity

Coding standards are essential to secure programming. Coding standards keep things simple, ensure that security is implemented in the program, and provides the assurance that other developers can understand the code with the least amount of confusion.

The most important ideal to remember when designing a secure application is simplicity. Creating the simplest solution to a problem usually means it will create the least amount of security issues. Overly complex code is much more difficult to secure. Keep in mind that in developing future versions of the application, or during bug fixes, developers who didn't initially write the code may be the ones trying to secure it.

Your code should not be secure by obfuscation because with enough time and determination, the obfuscation can be deciphered and exploited. Rather the security in the program should be very transparent and even modularized. This will allow the code that implements the security and has been proven to be secure to be reused in other areas of the program, and even in other software systems.

Principle of Data Protection

Hard-coding passwords into programs is probably the worst coding sin a developer can commit. Developers should never hard-code passwords into programs. If passwords are hard-coded into programs, it is possible that unauthorized users can discover them using sniffers or protocol analyzers, or even a simple Hex editor. Also, anytime a password or secure data is transmitted, the data should be encrypted with either a one way hash or some type of strong data encryption algorithm. An MD5 hash is a good example of this.

Principle of Distrust

All input is evil! This simple assumption will save you a lot of grief in the long run. Trusting a user to act in an expected manner is setting the security of the system up for failure. Because you cannot identify every type of input that may come your way, only allow what you know to be good through. This means that at every opportunity for the user to provide a value, click a button, open a file, or any other user interaction with the program, the input must be scrubbed. Until it is proven secure, the input cannot be trusted.

The simplest way to test user input is through simple exception handling. The means of doing this will change depending on the language you are using. Most object oriented languages employ a try/catch model of exception handling. Combine this with the use of regular expressions. Often times these two steps will stop all sorts of attacks including:

- Data format exceptions
- SQL injection attacks
- Buffer overflow attacks
- Stack pointer switches

The ultimate goal of secure programming is detecting and recovering from any unforeseen situation. This means

Secure Coding Principals

that if an error does occur during program execution, whether it was caused by bad user input or not, the application should handle the error in a kindly manner, or gracefully exit.

One thing to keep in mind when notifying a user that an error occurred is to not give away any information. A common example of this is with user login information. If an application tells the user that his password is incorrect when a correct username but a wrong password is entered and a different error message entirely when both are incorrect, this tells a malicious user that they have guessed a correct username. It may simply be a brute force guessing process to get a correct password; Hence, compromising the security of the entire system.

Lastly, the program should be secure by default. If an error or exception occurs and is caught, part of the graceful error handling should be to close open ports and database connections, release control of open files, and to overwrite the memory locations of secure data with null values.

S.T.R.I.D.E Principles of vulnerability

The acronym S.T.R.I.D.E describes all the different vulnerabilities a computer system may face. S.T.R.I.D.E stands for

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

Spoofing refers to various forms of falsification of data. Simply put, spoofing is pretending that you're someone you're not (i.e. someone trusted). Spoofing can take the form of using valid login information of a trusted person, a man in the middle attack where the communication between two entities is intercepted in both directions, or by changing HTTP referrer headers essentially fooling the system into thinking you are trusted.

Tampering simply means changing data. If tampering occurs through any means, security has been breached. Often tampering occurs when either an invalid user gains access to the system, or when information is intercepted in transit. Cryptographic hash functions and cryptographic signatures can be used to add a tamper-evident layer of protection to the data, often referred to as an electronic signature. A signed hash or Hex number is generated from the contents to be stored or transferred, and any change to the data, no matter how trivial, will cause it to have a different hash, which will make the signature invalid.

Repudiation simply means denial. This relates to secure coding principles usually through denial of responsibility. Repudiation must be prevented in all secure transactions. Proof of the integrity and origin of data and in the authentication of all users of a system are ways to prevent repudiation. This is especially important in eCommerce, legal contracts and exchanges, and other types of monetary transaction. Often times repudiation is used to circumvent the terms of a contract, and if identity cannot be proven the contract cannot be upheld.

Prevention of information disclosure is the main priority of secure coding. The principles and methods of doing so have already been discussed in this document.

Denial of service (DoS) attacks are all too common. A DoS is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. Denial of Service attacks can also lead to problems in the network 'branches' around the actual computer being attacked. For example, the bandwidth of a router between the Internet and a LAN may be consumed by a DoS, meaning not only will the intended computer be compromised, but the entire network will also be disrupted.

Elevation of privilege occurs when a trusted but restricted user gains access to data or programs which are meant only for system administrators or more privileged users. This obviously presents the same problems as the other exploits mentioned here. The exploits that a user uses to obtain an elevation of privilege cannot always be predicted. However like any other secure coding principle, this is one more thing to be aware of in the design and development process.

Secure Coding Principals

Conclusion

The secure programming principles need to be designed into your application from the very start and continuously evaluated throughout the development process. Not only does it make the applications being designed more robust and flexible, it ensures the safety and security of all programs, data, and the computer system or network. The basics of secure programming are to trust no user or input until it can be proven secure; common exploits must be known in order to take measures to prevent them; data protection is the most important purpose of secure coding; and if security cannot be ensured, then the program needs to take steps to recover or gracefully exit.

Hopefully, this has simplified what is to most people an incredibly complex subject. The fact-of-the-matter is that most beginning security mistakes can be solved by discontinuing lazy coding practices and creating a standard that is always followed. Most of today's security problems are caused by a combination of design flaws, poor programming standards, and programmer error.

This document is for informational purposes only. Tometa Software, Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.
Copyright © 2006 Tometa Software, Inc. All Rights Reserved.

Source: http://www.tometasoftware.com/secure_coding_principles.asp

Florida State Courts Requirements for SQL Server Database Development

1. Use CamelCase instead of underscores for object names.
2. Begin all names with a letter.
3. Do not use SQL Server reserved words by themselves as names (e.g., database, join, primary, begin, between)
4. Names should be as short as possible while remaining meaningful.
5. Table names should be singular.
6. A column name should be unique within the table.
7. Each table shall have a system generated unique identifier of type int or bigint using an ID suffix. (e.g., CaseID, CaseTypeLKID).
8. All Lookup or Code tables shall have a suffix of LK. (e.g., CaseTypeLK).
9. VARCHAR is to be used when the field values are of variable length. CHAR is used when the field values are fixed length. If unsure, use VARCHAR.
10. Names for Audit Columns: CreUser (not null), CreDate (not null), UpdUser ,UpdDate.
11. Trigger names: tU_<tablename> (Update trigger for table.) tD_<tablename> (Delete trigger for table.)
12. Stored Procedures prefix: SP; Functions prefix: FN
13. Use Active indicators or begin/end dates for all code/lookup tables.
<tablename>ActiveInd or <tablename>BeginDate, <tablename>EndDate.
14. Column constraints may be used for domains that are small and will most likely not change. (e.g., Gender, True/False (Yes/No)).
15. Some standard suffixes:

Code	A code that is known and used by a user to identify an Object.
ID	A system generated unique number used internally within the database and not usually known by the user. This is generated by using a table identity column.
Ind	Indicator column used to indicate the domain of the column has limited and/or Boolean values.
Date	Used for a date and date/time columns.

Best Practices, Design and Development guidelines for Microsoft SQL Server 2008

Madhu K Nair Jul 24, 2008

There are many resources available in the net but here I have a list of Best Practices, Design Guidelines and General Guidelines in Database Development and Designing specifically for SQL Server.

Best Practices

1. **Use Stored Procedure:** Benefits are as follows :-

- (a) Code reusability
- (b) Access Control: You can control permission on sp
- (c) Execution plan reusability : Though adhoc query also create and reuse plan, the plan is reused only when the query is textual match and the datatypes are matching with the previous call. Any datatype or you have an extra space in the query then new plan is created

Eg.

```
Select Sal from Employee where sal=$10 --Money
--And
Select Sal from Employee where sal=10 -- Int
```

Above statements will create different execution plan because the datatype of value is different.

- (d) Prevent SQL Injection
- (e) Procedure gives more Readability and Manageability.

2. **Use Fully Qualified Name for objects:** This is very significant. You must use fully qualified name when you refer any object in SQL Server. Ie. SchemaName.ObjectName. Because, when the execution plan is prepared by the query engine , in the binding process, Query engine has to resolve the Object existence. If you specify the fully qualified name the object resolution become easy for the engine and also it will be more readable.

3. **Avoid using Scalar Function in SELECT statement:** Recently I faced this issue and I emphasis this point. Never use Scalar function inside a query which returns a large number of rows. Scalar function behave like a cursor when you use Scalar function inside a query which returns large number of rows . Change the scalar function to Inline or Multiline table function or a view.

4. **Avoid Mixing-up DML and DDL statement on a temp table inside stored procedure:** This is very important. When you Create a temp table (#table) and ALTER the same temp table in the same stored procedure later, this DDL and DML mix-up causes the stored procedure to get recompiled. So, if a stored procedure is getting recompiled in each call check this point.

5. **Select only the required columns:** Select only the required column in select statement. Usage of SELECT * can be the cause of NOT using the indexes available on the table . Also if you are selecting more data then you are doing more IO. In short we should limit the IO.

6. **Avoid Usage of HINTS:** HINTS prevent Query engine automated optimization capability. You may find a hint gives you better performance on a particular scenario. But it may behave differently as the data grows or when scenario changes.
Check this KB on HINTS: <http://msdn.microsoft.com/en-s/library/ms187713.aspx>

7. **Use Table variable and Temp table as far as possible:** You must use Table variable (@TableName) or Temp table (#TableName) for intermediate storage of records in an procedure. Avoid using Table variable for large record set. There are pros and cons between Table variable and Temp table, but in general, if the record set is small you should go for Table variable.

8. **Use SET NOCOUNT ON :** Basically, you must reduce the data transferred on the network. Database Engine, return the number of rows effected by the statements to the client which is unnecessary and you can avoid that using this statement. It is a must in all Stored procedure.

9. **Do not change SET OPTION In connection:** Changing SET Option during connection or anywhere else

Best Practices, Design and Development guidelines for Microsoft SQL Server 2008

Madhu K Nair Jul 24, 2008

will cause the stored procedure to recompile. Refer this KB for more info:
<http://www.microsoft.com/technet/prodtechnol/sql/2005/recomp.msp>

10. **EXISTS vs IN** : IN Operator can easily be replaced by EXISTS which is more optimized for correlated queries. But you may find IN better for small tables.

11. **Keep the transaction as short as possible**: Deadlock is a outcome of ill-formed query. You must keep the transaction as short as possible to avoid dead lock. And also refer the object in the same order inside transaction.

12. **Avoid user input inside a transaction**: Do not accept a user input inside a transaction.

13. **Avoid doing Front-End work in Databases**: You should have a clear segregation of tasks between Data Layer, Data Access Layer (DAL) and Business Layer.

14. **Avoid Function in select statement**: Any functions like CONVERT(),CAST,ISNULL usage in query may ignore the indexes available on the table.

15. **Do not use EXEC ('String') , use sp_executeSql** : As far as possible you try to avoid Dynamic SQL. If there is no other option use sp_ExecuteSQL DO NOT USE EXEC('string'). Because EXEC statement is prone to SQL Injection and it is not parametrized query which can re-use execution plan.

16. **Use proper size for the input parameter**: This is one of the step to avoid SQL Injection and also the reduce the memory usage.

17. **Do not keep the name of sp with sp_ prefix**: Naming convention is very important. Do not name the storedprocedures with SP_ as prefix (eg sp_ somespname) because this naming convention is used for system stored procedure in MS SQL Server.

18. **USE WHERE Condition as far as possible**: Basically, you should limit the rows fetched by the query.

19. **Avoid Negative operator** : Avoid using <> , NOT IN, NOT EXISTS kind of operator because it causes a table scan. Query engine has to ensure there is not data till the last row is read.

20. **Avoid Cursor /loops**: In SET Based operation, in general looping can be avoided.

21. **Avoid using Like '% %'** : If you use % in both side of the searching value, the query will go for table scan which should be avoided. If the application is more text searching kind go for Full Text Index.

22. **Do not use WITH Recompile** : Usage of WITH Recompile causes the procedure to recompile each time it call. You must avoid this command.

23. **JOIN Consideration** : When you JOIN two table consider these points

- (a) Avoid using negative operator (<> ,NOT IN) in JOIN
- (b) Avoid Like operator in Join

Design Guidelines

1. **Create Covering indexes**: Create covering indexes. Covering index will have all the data required by the query at the leaf level itself. Covering contains all the columns used in SELECT, WHERE, ORDERBY, JOIN etc.

Eg.

```
Select Col1,Col2 From YourTableName Where Col3=1 Order by Col4.
```

The covering index for the above mentioned query will be

Col1+ col2+ col3+ col4. (Note : Most selective column should come first in the index creation statement)

Best Practices, Design and Development guidelines for Microsoft SQL Server 2008

Madhu K Nair Jul 24, 2008

2. **Remove Unwanted indexes** : In SQL Server 2005 it is very easy to find unused indexes. Too many or too less indexes on a table are equally bad. If you have unwanted/unused indexes on a table Insert/Update statement will have performance hit and also we all know indexes consume space.

3. **Create the indexes most selective column as first column in Index** : Index creation has to be done after proper analysis. You must create the index with Most Selective column at first and so on.

4. **Formatting the stored procedure and queries** : You must have a format / template for each object (sp/function/views) and everyone (the dev team) should stick to the format defined. And also the query has to be formatted well so that it is more readable.

5. **Use Identity column if the table is INSERT oriented table as Clustered Index to avoid page split**: This is a design and data modeling issue. If you have more insert kind of table (some kind of logging table) then you must go for Identity Column (ever increasing) as Clustered Index. This helps to resolve page split. There may be Hotspot issue (all transaction contending for same page of a table), but I have never faced.

6. **Use proper fill factor for Indexes**: Very important to avoid Page Split. In general transactional table can be kept at 80-90 fill factor.

7. **Balanced Normalization / De-normalization**: You must have a trade-off between Normalization and de-normalization. At time De-normalization can give you better performance at the cost of Data redundancy.

8. **Primary Key size and Composite primary key**: You must limit the size of the PK because, in a relational database, you may be creating foreign key which refers this primary key. If you have multiple Column in PK (composite PK) or big size, you are knowingly or unknowingly increasing the space usage. If the composite PK contains more than 3 columns then you may go for surrogate key like Identity column as PK.

9. **Do not alter system Objects**: If your application requires some tweaking of system objects then you are in trouble. The structure of system object can be changed by Microsoft in any release or patches. So avoid such modeling.

Guidelines for Datatype Selection

As a Database architect I believe in the significance of proper datatype selection while designing the tables. If you do a proper analysis of the data and then select the datatype, then you can control the row, page, table size and hence increase the overall performance of the database. Following points you may consider when you design a table :-

1. If your database is to support web-based application(s) it is better to go for UNICODE for the scalability of the application. (Unicode (nchar, nvarchar) takes 2 bytes per char where as ASCII (char, varchar) datatypes takes 1 bytes per char)

2. If your application is multi-lingual go for UNICODE.

3. If you are planning to include CLR Datatype (SQL Server 2005) in the database go for UNICODE

Best Practices, Design and Development guidelines for Microsoft SQL Server 2008

Madhu K Nair Jul 24, 2008

Datatypes , because, if CLR Datatype is going to consume the data then it must be in UNICODE.

4. For numeric column, find the range that column is going to have and then choose the datatype.

5. Description /Comments /Remarks sort of columns may or may not have data for all the rows. So it is better to go for Variable datatypes like Varchar ,Nvarchar.

6. If you know the column is not nullable and it may contain more or less the same size of the data then for sure go for Fixed datatype like CHAR or NCHAR. Having said that it is important to know that, if you select fixed datatypes and if the column is nullable then, if you do not have any data (null) then also the column will consume the space.

General Guidelines

1. **Write ANSI standard Code :** You must write standard code which will scale your application. ie migration to next version will not be an issue. Do not use Deprecated features.

2. **Do not give Error messages which exposes your architecture to the frontend:** I have seen folks give very detailed error message which tells you " blah blah table do not have this rows in blah blah database" kind which can be a invitation to the hacker.

3. **Use proper Isolation level required for the application:** This is very significant. Before going for any isolation level, you must know the implication. All application cannot afford READUNCOMMITTED Isolation level since it can cause data inconsistency issues like Dirty Read, Phantom read, Lost Update etc. WITH NOLOCK Hint is nothing but READ UNCOMMITTED isolation level.

4. **Keep the Database Object Scripts in Source Control:** We all are aware of this point but generally ignore. This is important for fault tolerance and management when multiple developers are working on same project.

Madhu K Nair:

<http://code.msdn.microsoft.com/SQLExamples/Wiki/View.aspx?title=ContributorBios&referringTitle=Best%20practices%20%2c%20Design%20and%20Development%20guidelines%20for%20Microsoft%20SQL%20Server&ANCHOR#MadhuKNair>