

**IT Professional Technical Services
Master Contract Program
T#:902TSSStatement of Work (SOW)
For Technology Services
Issued By**

**Minnesota Department of Public Safety, Bureau of Criminal Apprehension
Criminal Justice Training & Education (CJTE) Phase II
Web Design and Development**

*****Addendum*****

9/10/2010

- 1. How many individuals is BCA looking for to support this work?**

Two , or as many as are required to complete the work within the requested timeframe.

- 2. Does the past performance of at least two projects of a similar nature have to be past performance of specifically the vendor or can it be past performance of our proposed contractors?**

Specifically from the Vendor.

- 3. Can the three client solutions be from the proposed contractors as well?**

The client's solutions need to be from the Vendor.

- 4. Is offshore work an option to help contain costs?**

All work to be done on site.

- 5. Does the BCA require the work to be complete by 12/31/2010 or 1/31/2011 as identified in the Project Milestones and Schedule?**

All work to be completed by 1/31/2011.

- 6. How detailed are the requirements for the tasks you've identified in the RFP? What percentage complete are the requirements? Are you open to sharing them?**

Requirements identified in the RPF are functional requirements. No further details have been identified and will be developed in concert with the selected vendor. 100% to be completed by the project end date.

- 7. Can you please provide the Phase I CJTE system's project documentation specified below:**

**Screen shots of all screens in the system
List of batch processes
Requirements Specifications document
Data Model of the system
Technical Architecture model of the current system.**

See Attachment A below. This is a MOSS 2007 model.

8. Based on the URL provided for the CJTE system, it appears that it is a .web site using Microsoft .NET technologies. Please confirm.

The CJTE website is SharePoint 2007 based.

9. Please provide a list of functions that are currently available in the Phase I system so that we can assess the size and complexity of the enhancements in the context of the existing system functionality.

See Attachment A below.

10. In the link provided on page 4, the link is pointing to a PDF document containing the technical architecture standards. In that document, it is provided that the web application and data base integration will be achieved through J2EE (Java) technologies. Can you please confirm that the current system uses J2EE technologies?

The CJTE website is not a Java based.

11. Based on the Required Skills provided, it appears that the current system is developed in Microsoft Sharepoint environment using Sharepoint tools. Can you please confirm?

Correct.

12. On page 5, SOW states that the remaining functionality must be completed by January 31, 2011. However, below that it states that all work under this SOW must be completed by December 31, 2010. This seems to be contradicting. Can you please clarify?

All work to be completed by 1/31/2011.

13. Please indicate how many days of user acceptance time would be incorporate in the schedule for each of the three scheduled deliverable releases.

1-2 days needed per release.

14. Please indicate whether we must perform any load and performance tests based on the size and the concurrent access of the system.

Yes, would need to be evaluated but not deemed excessive at this time.

15. Please confirm whether we can propose to develop the system using an offshore delivery model using development facilities outside the US.

All work to be done on site.

16. Please confirm whether State will provide vendor team members' necessary work space and computer and network infrastructure to execute the project onsite at BCA facilities.

Workspace, computer and infrastructure can be provided for a limited number.

17. If remote development is used, will State provide VPN access to State development, test and production environment?

VPN may be provided on a limited basis.

18. Considering the number of enhancements provided in the SOW, we request you to kindly extend the proposal submission deadline to at least September 17th, 2010.

All proposals to be received by 2 p.m. CST on September 14, 2010.

19. Can we propose an alternate schedule, where by all project deliverables are completed by January 2011?

No.

20. Can you please provide the business driver for why the State wants certain deliverables on October 8th and November 1, 2010. Considering the nature of enhancements requirements, it may be infeasible to deliver any part of the new system by October 8, 2010.

Phased delivery preferred with deliverables based on proposed design and architecture and agreed to in final contract.

21. Are the Subject Matter experts who would provide detailed requirements for each enhancement located in BCA facilities in St, Paul? Do we have to travel to other State facilities to gather requirements?

All subject experts located at BCA HQ facility in St. Paul.

22. For receiving payments, does the current system have any integration with payment services for any credit cards? Please clarify.

There is no current 3rd party payment service design and is not needed in the development of this site. For purposes of this CJTE site, general invoicing and payment tracking are needed. Resources for 3rd party payments systems are external and would point to this CJTE site.

23. Please confirm the vendor deliverables listed in item 6 are updates to the existing documentation to the extent modified towards the new enhancements requested? Do these documents already exist or do we need to create these from scratch? If they already exist, can you please provide a copy of the existing version?

These do not exist and need to be created from scratch.

24. We could not locate Appendix B and C (pertaining to Non Visual Standards) although the SOW states that they have been attached and incorporated. Please provide the same.

Copies of Exhibit B and Exhibit C attached below.

25. Does the current system use a Relational database platform to store system records? If so, please provide the same.

The current records exist within SharePoint lists.

CJTE Theory of Operation

External Users - Anonymous users visit the CJTE site to obtain information on available training courses and to submit electronic forms requesting enrollment.

Internal Users (Training Coordinators) - Log on to the CJTE site to review and process registration requests.

SharePoint Workflows - Track enrollment levels and send email notifications to registrants based on the disposition of their requests.

Application Components

SharePoint Components

Aside from static informational content, the CJTE “application” consists of four primary lists and associated workflows:

- **AutoNumber** – List items contain sequence values which are incremented by workflows when Course or Schedule list items are created. Note: Values in this list must not be manually edited.
- **Course List** – List items contain course title, description, applicable fees, etc. and a unique Course Number.
 - Workflows:
 - “Create Course” – Assigns a Course Number and increments the associated sequence value in the AutoNumber list. Automatically started when a new item is created.
- **Course Schedule** – List items reference a Course Number and contain dates, location, seating capacity/filled, etc. and a unique Schedule Number.
 - Workflows:
 - “Create Schedule” – Assigns a Schedule Number and increments the associated sequence value in the AutoNumber list. Automatically started when a new item is created.
- **Course Registration** – List items reference a Schedule Number and contain registrant vital information, request status, etc.
 - Workflows:
 - “Reject Registration” - Changes status to Rejected. Manually started.
 - “Add to Waitlist” - Changes status to Waitlist. Manually started.
 - “Confirm Registration” - Changes status to Confirmed, increments Course Schedule seating filled, sends emails to registrant and supervisor. Manually started.
 - “Cancel Registration” - Changes status to Cancelled, decrements Course Schedule seating filled, sends email to registrant. Manually started.
 - “Reschedule Registration” - From a status of Pending or Cancelled, changes status to Confirmed, increments Course Schedule seating filled, sends emails to registrant and supervisor. Manually started. Takes a Schedule Number as input. Note: The workflow initiation form has been modified to take current username as hidden input which is validated via the workflow against the “Criminal Justice Training and Education Owners” group for authorization.
 - “Course Complete” – Currently unused.
- **RegistrationAdmin** – List items contain manually created hyperlinks to out-of-box and custom pages and comprise a menu system accessible only by authenticated users.
 - Workflows:
 - None

Exhibit B

Department of Public Safety's Security Architecture

Minnesota Department of Public Safety divisions and their vendors should be aware of the department's security architecture when designing and/or implementing applications or installing network devices on departmental resources.

Web Based Applications and/or Servers

Web Based Applications should be based upon Microsoft Internet Information Server unless there is compelling business needs to use some other Web Server environment.

Web Servers will be installed on a separate and isolated Ethernet network segment behind a departmental firewall.

Web Servers must not host Applications. Applications must reside on a separate Application Server on a separate and isolated Ethernet network segment behind a departmental firewall.

The departmental network is TCP/IP based.

As the default profile of the firewall is to deny all incoming and outgoing traffic, DPS divisions and/or their vendors must provide all source and destination addresses, port numbers, and protocols required for network communications. In addition, they must provide a written business need for the network communications.

Database Applications and/or Servers

Database Applications should be based upon Microsoft SQL Server unless there are business needs to use some other Database Server environment.

Database Servers will be installed on a separate and isolated Ethernet network segment behind a departmental firewall.

The departmental network is TCP/IP based.

As the default profile of the firewall is to deny all incoming and outgoing traffic, DPS divisions and/or their vendors must provide all source and destination addresses, port numbers, and protocols required for network communications. In addition, they must provide a written business need for the network communications.

Email Based Applications and/or Servers

DPS divisions and/or their vendors are encouraged to use the department's email system where appropriate.

Email Based Applications should be based upon Microsoft Exchange Server unless there is compelling business needs to use some other Web Server environment.

Email Servers will be installed on a separate and isolated Ethernet network segment behind a departmental firewall.

The departmental network is TCP/IP based.

As the default profile of the firewall is to deny all incoming and outgoing traffic, DPS divisions and/or their vendors must provide all source and destination addresses, port numbers, and protocols required for network communications. In addition, they must provide a written business need for the network communications.

Applications and/or Application Servers

DPS divisions and/or their vendors will need to discuss with the departmental Security Manager as to the appropriate placement of applications and application servers.

Data Privacy

Since some departmental data is classified as “Not Public” data, this type of data must be protected during transport across public networks and possibly in storage.

The department has implemented Virtual Private Network (VPN) technology to aid in the transport of private data.

Contact the departmental Security Manager for discussions on the use of this technology.

Vendor Remote Access

Remote vendor access for technical support will occur when there is a valid business need, through a secured and monitored VPN. If persistent access is required, the VPN will use two-factor authentication. If one time access is required, VPN access may be granted using a strong password. This remote VPN access shall be limited by the firewall and/or VPN server to the specific protocols, ports, and servers needed.

Vendor staff may be required to undergo a background criminal history check in accordance with DPS Policy #5100 Information Resources Security and Acceptable Use.

(THE REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK)

Exhibit C

Non-Visual Access Standard

Nonvisual access standards require:

- 1) The effective interactive control and use of the technology, including the operating system, applications programs, prompts, and format of the data presented, are readily achievable by nonvisual means;
- 2) That the nonvisual access technology must be compatible with information technology used by other individuals with whom the blind or visually impaired individual must interact;
- 3) That nonvisual access technology must be integrated into networks used to share communications among employees, program participants, and the public; and
- 4) That the nonvisual access technology must have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.
- 5) Nothing in this section requires the installation of software or peripheral devices used for nonvisual access when the information technology is being used by individuals who are not blind or visually impaired.

(THE REMAINING PORTION OF THIS PAGE WAS INTENTIONALLY LEFT BLANK)