

**IT Professional Technical Services
Master Contract Program
902TS
Statement of Work (SOW)
For Technology Services
Issued By
Minnesota Department of Public Safety
Bureau of Criminal Apprehension**

**Project Title: 2nd REPOST for Microsoft System Center
Operations Manager (SCOM) Production Environment
Deployment
Service Category: Technical Analyst**

Business Need

The Minnesota Bureau of Criminal Apprehension Minnesota Justice Information Services (MNJIS) requires Microsoft System Center Operations Manager (SCOM) expertise to review its existing Microsoft SCOM implementation, make recommendations for tuning and extending its current implementation, assist in further configuration and implementation, and provide knowledge transfer to BCA MNJIS Network Operations staff.

The mission of the BCA is to protect Minnesotans and all who visit our state by providing services to prevent and solve crimes in partnership with law enforcement, public safety and other criminal justice agencies. The MNJIS division supports the mission of our criminal justice partners, namely through facilitating access and the exchange of information between sources of criminal justice data. The Microsoft System Center Operations Manager implementation will provide information and alerting to ensure the timely and reliable delivery of information services to our criminal justice partners.

Project Deliverables

This project resource for this project will provide SCOM expertise, including:

1. Reviewing existing test and production deployment design:
 - a. Validate identified system and service monitoring requirements.
 - b. Report on any issues not meeting Microsoft best practice.
 - c. Recommend tuning of existing test and production deployments.
 - d. Making recommendations for using Microsoft SQL Management Pack and Microsoft Cluster Management Pack.
 - e. Recommend third-party management packs and configuration for monitoring non-Windows servers and VMware virtual servers.
2. Making recommendations for and configuring service/distributed application monitoring:
 - a. Configure end-to-end monitoring for two (2) Test and Production MNJIS distributed applications/services.
 - i. One service based primarily on MS Windows Server Platform and .NET architecture.
 - ii. One service based primarily on Red Hat Linux and J2EE.

- b. Assist with end to end testing of new distributed application implemented
 - c. Create at least one synthetic transaction running against .NET web applications.
 - d. Produce reports for each of the two distributed applications/services created to show the performance and availability of these services.
- 3. Validating and improving alerting design, including recommendations for:
 - a. Alert groups.
 - b. Information to be included in alerts.
 - c. Alert overrides where applicable.
- 4. Creating central dashboard views for servers and distributed applications being monitored by SCOM.
- 5. Designing and assisting with configuration of Service Level Dashboard (SLD 2.0) for real-time monitoring.
- 6. Creating Operations Manager Reporting Service reports.
 - a. Recommend reports to be used by Operations staff and by management.
 - b. Configure and publish at least five (5) SCOM reports based on the SCOM generic reports library.
- 7. Providing knowledge and skills transfer to BCA MNJIS technical staff.
- 8. Documenting all recommendations and configuration changes.

Specific deliverables required are:

- 1. Reports documenting:
 - a. Current SCOM implementation compliance with Microsoft best practices.
 - b. Tuning recommendations for current SCOM implementation.
 - c. Requirements validation for system and service monitoring.
 - d. Recommendations for SQL Management Pack and Microsoft Cluster Management Pack use.
 - e. Recommendations for third-party management packs and configuration for monitoring non-Windows servers and VMware virtual servers.
 - f. Any other recommendations for system tuning or enhancement.
 - g. All configuration changes made to the system as a result of the recommendations.
- 2. Assistance with tuning and configuration, including:
 - a. Configuration of at least two (2) Test and Production MNJIS distributed applications/services.
 - i. One service based primarily on MS Windows Server Platform and .NET architecture.
 - ii. One service based primarily on Red Hat Linux and J2EE.
 - b. Reports for each of the two distributed applications/services created to show the performance and availability of these services.
 - c. End to end testing of distributed application.
 - d. Creation of synthetic transaction for .NET web application.
 - e. Central dashboard views for monitoring servers and distributed applications.
 - f. Service Level Dashboard 2.0.
- 3. Knowledge and skills transfer for BCA MNJIS technical staff in SCOM administration and best practices. This will be completed by working with MNJIS technical staff to configure and implement SCOM.

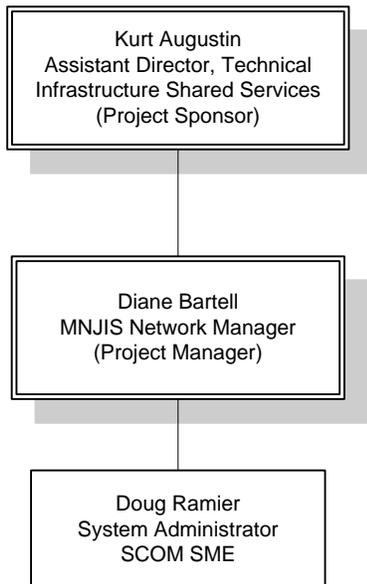
Contractor must perform and provide all services, tasks, and deliverables for this project to the State in accordance with the "State of Minnesota Enterprise Architecture" available to the Contractor on website <http://mn.gov/oet/policies-and-standards/enterprise-architecture/index.jsp> in accordance with the Department of Public Safety's Security Architecture labeled Exhibit A which is attached and incorporated into this Statement of Work, and in accordance with the "Minnesota Office of Technology's Minnesota Electronic and Information Technology Accessibility" guidelines available to the Contractor on website <http://mn.gov/oet/policies-and-standards/accessibility/>

Project Milestones and Schedule

- Estimated Engagement Start Date
 - Monday, March 28, 2011.
- Project Completion Date:
 - Thursday June 30, 2011.

Project Environment (State Resources)

- Staff descriptions:
 - a) Project Sponsor: Kurt Augustin
 - b) Project Manager: Diane Bartell
 - c) Operations Subject Matter Experts (SMEs): Doug Ramier
- Basic organizational structure (organizational chart) of the project, see below



- Staff proficiency levels and experience (with methodology, tools, etc.)

Doug Ramier – 1 year of experience working with Microsoft Systems Center Operations Manager; several years of experience with other monitoring tools, such as InterMapper,

Project Requirements

- System implementation will be performed onsite at the BCA facility at 1430 Maryland Ave E, St. Paul, Minnesota.
- Successfully passing the BCA Background Check will be a condition of accepting the resource.
- Significant training of BCA staff will be required for the rollout of a new toolset for Release and Deployment Management. Thorough planning for training, including but not limited to, customization, content determination, and scheduling, will need to be performed.
- The resource selected from this Statement of Work will work with BCA contract vendors and staff to implement upgrades and updates to the system.
- Compliance with Minnesota Statewide Project Management Methodology.
- Compliance with BCA MNJIS project management and software development methodology.
- Compliance with applicable industry/agency standards.

Required Skills

Technical Skills:

- Technical resource must have completed at least two similar engagements, with demonstrably similar requirements, to the satisfaction of the customer(s).
- At least two years of experience administering and tuning Microsoft System Center Operations Manager 2007.
- Two or more years of experience designing and managing Microsoft Windows Server 2005 or 2008 server systems, including experience administering: IIS, Windows Clustering Services, DNS infrastructures, Active Directory.
- One or more years of scripting experience, including WMI, PowerShell, VBscript, and Linux Bash scripting.

Business Skills:

- Ability to understand business drivers and relate them with technical implementation work.
- Ability to prioritize business requirements to deliver maximum value.
- Ability to drive change to business process in the organization.
- Planning, organizing, and reporting experience.
- Process design, implementation, and optimization experience.
- Customer-focus and results orientation.
- Ability to work with other contract vendors as needed.

References

Provide three (3) references for resource from similar prior engagements. These contacts should be from the firm or agency where the engagement was performed, not from contract firm. Contact may be peer, manager, or supervisor on site. Provide the following contact information:

- Contact name, title, and phone
- Firm or Agency and name of project
- Dates and role on the project

Process Schedule

- Deadline for Questions 2/28/2011, 2:00 p.m. CST
- Posted Response to Questions 3/02/2011, 2:00 p.m. CST
- Proposals due date 3/03/2011, 2:00 p.m. CST
- Anticipated proposal evaluation begins 3/04/2011, 9:00 a.m. CST
- Anticipated proposal evaluation & decision 3/18/2011, 2:00 p.m. CST

Questions

Any questions regarding this Statement of Work should be submitted via e-mail by 2/28/2011, 2:00 p.m. CST.

Name: Maureen Janke
Department: Department of Public Safety, Bureau of Criminal Apprehension
Telephone Number: 651-793-2720
Email Address: maureen.janke@state.mn.us

Questions and answers will be posted on the Office of Enterprise Technology website by 3/03/2011, 2:00 p.m. CST (www.oet.state.mn.us).

Response Requirements

Vendor must have been previously qualified for the 902TS program with OET's Master Contract Program and be qualified in the Technical Analyst resource type.

One copy of the following for each Vendor presenting resources: Attach these documents to the Original overview cover letter and have it signed by an officer of the company.

- Company overview cover letter (limit to two (2) pages). Ensure items below are identified.
 - a) Company history, growth
 - b) Current financial data if publicly available
 - c) Description of the Vendor's understanding of the need and explanation of their proposed solution.
 - d) Conflict of interest statement as it relates to this project
- Required forms to be returned that must be included in proposal
 - a) Affidavit of non-collusion
<http://www.mmd.admin.state.mn.us/doc/noncollusion.doc>
 - b) Location of Service Disclosure
<http://www.mmd.admin.state.mn.us/Doc/ForeignOutsourcingDisclosureCertification.doc>
 - c) Certification Regarding Lobbying
<http://www.mmd.admin.state.mn.us/doc/lobbying.doc>
 - d) Veteran-Owned/Service Disabled Veteran-Owned Preference Form (if applicable)
<http://www.mmd.admin.state.mn.us/doc/vetpref.doc>
 - e) Minority or woman owned company (if applicable)

Each candidate resource being presented by a Vendor must be submitted with one "Original" included with the Vendor's background information as stated above; three hard copies and one electronic (C.D. or thumb drive) copy

- 1) Resume of candidate
- 2) References of candidate: Provide three from similar engagements (see instructions above).
- 3) Hourly rate of Technical Analyst resource

Proposal Submission Instructions

- Response Submittal Information:
 - a) BCA/MNJIS
 - b) 1430 Maryland Avenue East, St. Paul, MN 55106
 - c) Label the response Attention: Maureen Janke – Response to Release and Deployment Business Analyst
- Submit in person to BCA front desk receptionist or by mail by response deadline of 2/23/2011, no later than 2:00 p.m. CST.
- Number of copies 1 original, 2 copies, 1 electronic copy
- Key dates:
 - a) Response due date – 3/03/2011 no later than 2:00 p.m. CST.
 - b) Vendor's price/terms guarantee must be valid for the length of the engagement.
 - c) No other person than Maureen Janke is authorized to answer questions regarding this Statement of Work. All vendors are to follow the above instructions regarding posting questions only to the named contact.

SOW Evaluation Process

Responses will be scored accordingly

- Experience of resource with similar project engagements (30%)
- Skills as defined in "Required Skills" section above (30%)
- References of candidate (10%)
- Cost (30%)

General Requirements

Proposal Contents

By submission of a proposal, Responder warrants that the information provided is true, correct and reliable for purposes of evaluation for potential award of this work order. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the responder to suspension or debarment proceedings as well as other remedies available by law.

Indemnification

In the performance of this contract by Contractor, or Contractor's agents or employees, the contractor must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the state, to the extent caused by Contractor's:

- 1) Intentional, willful, or negligent acts or omissions; or
- 2) Actions that give rise to strict liability; or
- 3) Breach of contract or warranty.

The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligation under this contract.

Disposition of Responses

All materials submitted in response to this SOW will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the selected vendor. If the Responder submits information in response to this SOW that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, the Responder must: clearly mark all trade secret materials in its response at the time the response is submitted, include a statement with its response justifying the trade secret designation for each item, and defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments or damages awarded against the State in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State's award of a contract. In submitting a response to this SOW, the Responder agrees that this indemnification survives as long as the trade secret materials are in possession of the State.

The State will not consider the prices submitted by the Responder to be proprietary or trade secret materials.

Conflicts of Interest

Responder must provide a list of all entities with which it has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request for proposals. The list should indicate the name of the entity, the relationship, and a discussion of the conflict.

The responder warrants that, to the best of its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to organizational conflicts of interest. An organizational conflict of interest exists when, because of existing or planned activities or because of

relationships with other persons, a vendor is unable or potentially unable to render impartial assistance or advice to the State, or the vendor's objectivity in performing the contract work is or might be otherwise impaired, or the vendor has an unfair competitive advantage. The responder agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to the Assistant Director of the Department of Administration's Materials Management Division ("MMD") which must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. If an organizational conflict of interest is determined to exist, the State may, at its discretion, cancel the contract. In the event the responder was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to MMD, the State may terminate the contract for default. The provisions of this clause must be included in all subcontracts for work to be performed similar to the service provided by the prime contractor, and the terms "contract," "contractor," and "contracting officer" modified appropriately to preserve the State's rights.

IT Accessibility Standards

Responses to this solicitation must comply with the Minnesota IT Accessibility Standards effective September 1, 2010, which entails, in part, the Web Content Accessibility Guidelines (WCAG) 2.0 (Level AA) and Section 508 Subparts A-D which can be viewed at:

http://www.mmd.admin.state.mn.us/pdf/accessibility_standard.pdf

Nonvisual Access Standards

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.

Preference to Targeted Group and Economically Disadvantaged Business and Individuals

In accordance with Minnesota Rules, part 1230.1810, subpart B and Minnesota Rules, part 1230.1830, certified Targeted Group Businesses and individuals submitting proposals as prime contractors shall receive the equivalent of a six percent preference in the evaluation of their proposal, and certified Economically Disadvantaged Businesses and individuals submitting proposals as prime contractors shall receive the equivalent of a six percent preference in the evaluation of their proposal. Eligible TG businesses must be currently certified by the Materials Management Division prior to the solicitation opening date and time. For information regarding certification, contact the Materials Management Helpline at 651.296.2600, or you may reach the Helpline by email at mmdhelp.line@state.mn.us. For TTY/TDD communications, contact the Helpline through the Minnesota Relay Services at 1.800.627.3529.

Veteran-owned/Service Disabled Veteran-Owned Preference

In accordance with Laws of Minnesota, 2010, Chapter 333, Article 2, Section 3, Subdivision 6a, eligible certified veteran-owned businesses, with their principal place of business in Minnesota and Center for Veteran Enterprises verified (CVE Verified) by United State Department of Veterans Affairs, will receive up to a 6 percent preference in the evaluation of their proposal.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses include certified small businesses that are majority-owned and operated by either recently separated veterans, veterans with service-connected disabilities, and any other veteran-owned small businesses (pursuant to Laws of Minnesota, 2010, Chapter 333, Article 2, Section 3, Subdivision 6a).

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses must be **currently** certified by the U.S. Department of Veterans Affairs (in accordance with Public Law 109-461 and Code of Federal Regulations, title 38, part 74) prior to the solicitation opening date and time to receive the preference.

Information regarding certification by the United States Department of Veterans Affairs may be found at <http://www.vetbiz.gov>.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses should complete and **sign** the **Veteran-Owned/Service Disabled Veteran-Owned Preference Form** in this solicitation. Only eligible, certified, veteran-owned/service disabled small businesses that provide the required documentation, per the form, will be given the preference.

Foreign Outsourcing of Work Prohibited

All services under this contract shall be performed within the borders of the United States. All storage and processing of information shall be performed within the borders of the United States. This provision also applies to work performed by subcontractors at all tiers.

Statement of Work does not obligate the state to award a work order or complete the assignment, and the state reserves the right to cancel the solicitation if it is considered to be in its best interest. The Agency reserves the right to reject any and all proposals.

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

Exhibit A

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)