

Agency IT Procurement Review Guidelines

June 3, 2009

Purpose

The State Procurement Bureau (SPB) in conjunction with the State CIO, issued new delegated purchasing authority to agencies on October 1, 2007. Included in this agreement was section 11.2 dealing with information technology. These guidelines are intended to assist agencies in the use of this delegation.

Agency Roles & Responsibilities

Agency Director: The department head of an executive branch agency or organization is ultimately responsible for compliance with terms and conditions of their delegated purchasing agreement and this procedure.

Procurement Delegation Liaison: The procurement delegation liaison, as identified in the State Procurement Bureau (SPB) Procurement Delegation Agreement, is responsible for performing the agency review, ensuring the IT procurement conforms to state policy, standards, plans and architectures, and submitting the log of IT activities and procurements to Information Technology Services Division (SITSD.)

An agency is authorized to further delegate this procurement authority within their agency as outlined in section 5.1 of their Procurement Delegation Agreement.

Contract signing authority under this procedure allows contracts/agreements, which fall under the agency delegated authority of under \$25,000, to be signed for the CIO by the agency, according to the agency's signing authority. This does not extend to contracts or amendments which are part of a larger project, or to contract amendments which take the total cost of the project over \$25,000. These must be submitted to SITSD for review.

Agencies must comply with all Title 18 procurement laws and practices, terms of the delegation agreement as clarified by these guidelines. Agencies are responsible:

- For ensuring the quality of the Requests for Proposals (RFPs), contracts, Statements of Work (SOWs) or other related procurement vehicles. This includes ensuring that all standard SITSD language is contained in the document(s)
- For ensuring an adequate level of security for all data within the department and shall include appropriate security requirements, as determined by the department, in written specifications for the department's solicitation of data and information technology resources
- For ensuring an adequate level of consideration is given to the impact that the acquisition of an IT activity will have on the security and operation of the state network
- For maintaining the auditable records of their review and approval
- For maintaining a log of acquisitions made under this delegated authority, and submitting the log to SITSD on a monthly basis

ITPRs must still be submitted to SITSD for review and approval if the IT procurement is in excess of \$25,000 or is listed as one of the exceptions to the agency delegated authority in Appendix A. Procurements needing ITPRs would include such items as software not listed on the Accepted Software Products list, collaboration tools, monitoring tools, duplication of enterprise services or infrastructure, among others. Please review the Appendices of these guidelines for more details.

Process

Agency staff will present their IT activities and procurement requests to the agency Procurement Delegation Liaison for consideration. The agency Procurement Delegation Liaison must review the request to ensure it complies with terms of the delegation agreement. The agency Procurement Delegation Liaison will make a determination on whether the request can be handled by the agency as directed in this document, and if so, log the requests in an Excel spreadsheet using the log template provided by SSITSD. If it is determined the procurement doesn't fall within the agency delegated authority, the request will be submitted to SITSD for review. See Appendix D.

Agencies which are exempt per MITA

The following agencies as identified in section 2-17-516 of the MCA are exempt from these procedures as outlined below: University System, Office of Public Instruction and National Guard.

- (1) Unless the proposed activities would detrimentally affect the operation of the central computer center or the statewide telecommunications network, the office of public instruction is exempt unless specifically mentioned in section 14 of HB-4.
- (2) Unless the proposed activities would detrimentally affect the operation of the central computer center or the statewide telecommunications network, the university system is exempt unless specifically mentioned in section 14 of HB-4.
- (3) The National Guard, as defined in section 10-1-101 of the MCA is exempt unless specifically mentioned in section 14 of HB-4.

Requests for a change or exception to this procedure are made by emailing ITrequests@MT.gov.

Appendix A

Items that do not fall under the Agency Delegated Authority, even though it costs less than \$25,000

1. Infrastructure Duplication

On April 25, 2006 the CIO and Budget Director issued *Guidelines for IT Infrastructure Purchases*. The guidelines were intended to avoid duplication of IT resources during the period prior to the construction of new service centers. The following procurements may not use the Agency Review process and delegated authority. These procurements must receive prior approval by SITSD:

- a. SANS
- b. Servers
- c. Tape units
- d. Backup facilities
- e. Backup software or services
- f. Data center building and expansions
- g. Environmental protections for existing data centers (generators, fire suppression, security, HVAC etc)

2. Product Compliance

Products that are not in compliance with State policies and standards or are not approved on the State Accepted Software Products list must be submitted to SITSD via an ITPR to receive an approval for an exception prior to purchase. (Note, some products are on the list but still require an ITPR.) Additional licenses of “Off the Shelf” software previously approved through the ITPR process do not require an ITPR for that agency, so long as it is the same version which was previously approved. The agency must provide the previously approved ITPR number in their Agency Review log. Any restrictions or conditions in the original approval would still apply to subsequent purchases. Any additional licenses or modifications to a previously approved exception, requires an ITPR.

Current state policies and standards for hardware, software, architecture and security can be found in the following link:

<http://sSITSD.mt.gov/service/support/enterprisearchitecture.aspx#DNNsoftware>

3. Duplicate Products

Products that duplicate enterprise services provided by SITSD may not be handled via the Agency Review process and delegated authority. This includes, but is not limited to:

- a. Microsoft’s Identity Integration Server or other identity management software
- b. Email server software
- c. Citrix presentation software or gateway appliances for network access
- d. Active directory products and services
- e. Document or content management systems

- f. Communications network equipment (routers, switches, firewalls, hubs, access points, trunk lines, etc)
4. Collaboration Tools or other potential heavy bandwidth uses

Collaboration tools, video streaming or similar activities may introduce network and security risks and must receive approval prior to purchase. These tools may include, but are not limited to:

- a. Instant Messaging (IM), white board
- b. Go-to-MyPC, Peer to peer document sharing
- c. Desktop sharing tools
- d. IP based telephony or voice conferencing
- e. Streaming video or audio
- f. Social networking tools (Twitter, Linked, Facebook, MySpace)

Please review Appendix C for details of what information is required in the ITPR.

5. Modifications to Contracts or Statements of Work, which have previously been approved by SITSD, even though the modification falls under \$25,000 or amendments which push the total contract value above \$25,000, still require an ITPR and review by SITSD.
6. Other **Prohibited** practices
- a. Network tools (i.e., network sniffer)
 - b. Security "hacking" tools
 - c. Extreme bandwidth utilization
 - d. Security risk as per NIST
 - e. Server monitoring tools

Appendix B

IT Activity above \$25,000, yet still falls within the Agency Delegated Authority

Agencies have been and continue to be authorized to review and approve the acquisition of IT resources through procurement that exceed \$25,000 provided it falls within one of the following categories:

1. State standard PC's, laptops, and other portable computing devices purchased from a state term contract and which comply with State Hardware Standards. This includes all PC peripheral hardware such as memory, disk, PC printers, monitors etc
2. Hardware maintenance renewals **except:**
 - a. Maintenance on non-standard hardware
 - b. Maintenance on hardware that has been granted a conditional exception to State standards
 - c. Maintenance that includes additional hardware or hardware upgrades other than those in the initial approval by SITSD.
 - d. Maintenance of servers not previously approved through the ITPR process
3. Software maintenance renewals **except:**
 - a. Contracted consulting services for ongoing maintenance, modifications, or customizations
 - b. Maintenance for software products that have been granted exceptions to State Accepted Software Products list
 - c. Maintenance to software products, which are not in compliance with the State Accepted Software Products unless specifically delegated for a specific period of time
 - d. Maintenance procurements that include version/release upgrade licenses
 - e. Maintenance under a new contract/ agreement or amended contract/agreement which has not been reviewed and approved by SITSD
4. All embedded intelligent devices provided the data is not uploaded or downloaded into the agency's IT system, and the embedded devices or systems do not use the State's network for communications
5. All information technology education classes that are a standard offering (fixed times, published schedule, quoted prices, etc.) from an established vendor, that do not require a contract or statement of work. PC based software that is designed for IT training, and that does not use the State's network must still be reviewed with SITSD's Training Coordinator before purchase

Appendix C

ITPR Guidance

Issues that SITSD typically looks for in their review of ITPRs

1. WEB
 - a. ePass Montana
 - b. State Electronic Payment Processing Portal
 - c. State Web standards
 - i. mt.gov Template Standard
 - ii. eGovernment Services Certification Standard
 - d. Accepted software

2. GIS
 - a. Has the state GIS bureau reviewed any GIS component of a project or IT activity?

3. Network issues
 - a. Bandwidth consumption
 - i. A detailed Technical description of the device, application, or service
 - ii. Web Site address for the device, application, or service
 - iii. Number of devices (average and maximum anticipated) that will be connected to or accessing the device, application, or service
 - iv. Physical street address of each device connecting to or accessing the device, application, or service
 - v. Bandwidth requirements on average and maximum for each device connecting to or accessing the device, application, or service
 - vi. Describe the frequency of use, average amount of time of use for each device, application, or service will be utilized including the time of day and how often
 - vii. Timeline for implementation or typical schedule of use.
 - b. Network Hardware and software managed by SITSD
 - i. Use of network or server monitoring systems

4. Security.
 - a. Is there an agency information security plan referenced for the information system that the product or service acquisition is a component of?
 - b. If the acquisition is a component of an entirely new information system in the organization, has the information security plan been completed for the new information system?

The questions that should be addressed by an IS Security plan include but are not limited to:

- a. a categorization of all the information in the system
 - b. an information risk assessment on the system
 - c. a recommended set of security controls (mitigation plan)
 - d. plan of action and milestones for planned future controls
 - e. the identification and analysis of the common controls provided by any third party service provider
 1. Agency data security
 2. Enterprise Vulnerability
 3. Network Vulnerability
 4. Server Vulnerability
 5. Database Vulnerability
 6. Application Vulnerability
5. Video and Collaboration tools (Microsoft OfficeLive, WebEx, etc.)
- a. Bandwidth
 - b. Security of data and of the enterprise infrastructure
 - c. Existing contract? (MetNet)
6. Software/Hardware Standards
- a. Accepted products
 - b. Exclusive contracts for procurement
 - c. Servers, SANS, back up systems - look at SITSD service provision as an option in your business case
7. Enterprise services and infrastructure duplication
- a. Servers, SANS, back up systems - look at SITSD service provision as an option in your business case
 - b. Computer room builds
8. Contracts/SOW
- a. Clear deliverables
 - b. Payment plan (set asides/holdback)
 - c. Clear Roles and Responsibilities
 - d. Detailed completion and final acceptance criteria
 - e. Language which ensures all tasks and deliverables will get completed within an amount not to exceed \$_____
 - f. CIO signatory
9. Significant projects should involve the PMO early (complete project Ideation)
- a. More than \$250,000 or
 - b. High Complexity and/or
 - c. High risk exposure and/or
 - d. Politically Sensitive
10. Policy or Standards Exception Request
- a. Separate process
 - b. Submit the exception request at the same time as the ITPR

11. Time Constraints

- a. The more time invested in early work, such as requirements and planning, the quicker the review and approval
- b. Recognize that SITSD gets requests from all state agencies and there may be a backlog of requests, so please build adequate time into your schedule to allow for two to three weeks, especially if there are some questions or concerns which need to be worked out between SITSD and the agency
- c. If SITSD subject matter expert (SME) input is needed and has not been vetted prior to submission, this may delay the review process while SME's have a chance to review. Contact the itrequests@mt.gov mail address to find out which SME might be able to guide you
- d. If there is a critical time constraint for your project, you may want to make a call to the ITPR review analyst(s) in addition to submitting the request to the itrequests@mt.gov mailbox to give them a heads up. Also, be sure to be specific in the ITPR with a date and the reason for the urgency of the request

12. Procurement Law

- a. Is your project/procurement in compliance with procurement law Title 18 MCA?

Appendix D

Agency Log Format

The log **Filename** should include the month (three letter abbreviation) and year of the submission. Eg. DOA Log MMMYY as in DOA Log OCT08 (see Appendix E).

Cumulative activity for the State FY should be included in the monthly log submission. A new log will be started with each State fiscal year .

The log captures the essential information about the procurement (The log template is available from SITSD). The data fields in the spreadsheet include:

- Agency Assigned ITPR number (ex. DOAYYMM (seq#) or DOA0810123 or a numbering system of the agency's choosing)
- Agency code (standard 3 digit code; DOR, DOA, MDT, etc.) see Appendix E
- Agency Contact who approved the request
- Date approved (approved by the agency)
- Description
- Vendor
- Cost
- Agency Contact making the request
- Agency Review category
 1. PC and Peripherals
 2. Hardware maintenance renewal
 3. Software maintenance renewal
 4. Embedded device
 5. Education
 6. Accepted software products list- < \$25,000 and listed as not requiring an ITPR
 7. Additional Licenses
- SITSD assigned ITPR number for related procurements previously approved, allowing for agency authority of categories 2, 3 and 7(listed in the previous field)

Agencies must email a copy of their State FY cumulative log to itrequests@mt.gov by the 10th of each month.

SITSD will review the agency logs each month for compliance with this procedure. Additional information may be requested about the procurement, product, service, or activity.

Appendix E

Agency Abbreviations

| | |
|-----|--|
| ADV | Montana Advocacy Program |
| AGR | Department of Agriculture |
| ART | Montana Arts Council |
| BOE | State Board of Education |
| BPE | Board of Public Education |
| CHE | Office of the Commissioner of Higher Education |
| COR | Department of Corrections |
| CPP | Commissioner of Political Practices |
| DEQ | Department of Environmental Quality |
| DLI | Department of Labor and Industry |
| DMA | Department of Military Affairs |
| DNR | Department of Natural Resources & Conservation |
| DOA | Department of Administration |
| DOC | Department of Commerce |
| DOJ | Department of Justice |
| DOR | Department of Revenue |
| FWP | Department of Fish, Wildlife and Parks |
| GOV | Governor's Office |
| HCT | MSU Helena College of Technology |
| HHS | Department of Public Health & Human Services |
| HIS | Montana Historical Society |
| ISD | Information Technology Services Division |
| JUD | Judiciary |
| LEG | Legislative Branch |
| LIV | Department of Livestock |
| LOT | Lottery |
| MDT | Department of Transportation |
| MSL | Montana State Library |
| OPI | Office of Public Instruction |
| PER | Public Employees Retirement |
| PSC | Department of Public Service Regulation |
| SAO | State Auditor's Office |
| SDB | Montana School for the Deaf and Blind |
| SOS | Secretary of State |
| STF | Montana State Fund |
| TRS | Teachers Retirement |
| USM | University System |