Office of the Washington State Auditor

Pat McCarthy

Whistleblower Investigation Report

Department of Health

Published February 16, 2017

Report No. 1018638

Office of the Washington State Auditor
Pat McCarthy

February 16, 2017

John Wiesman, Secretary of Health
Department of Health

Report on Whistleblower Investigation

Attached is the official report on Whistleblower Case No. 16-016 at the Department of Health.

The State Auditor's Office received an assertion of improper governmental activity at the Department. This assertion was submitted to us under the provisions of Chapter 42.40 of the Revised Code of Washington, the Whistleblower Act. We have investigated the assertion independently and objectively through interviews and by reviewing relevant documents. This report contains the result of our investigation.

Questions about this report should be directed to Whistleblower Manager Jim Brownell at (360) 725-5352.

Sincerely,

Pat McCarthy

State Auditor

Olympia, WA

cc: Governor Jay Inslee
Lynda Karseboom, Internal Auditor
Kate Reynolds, Executive Director, Executive Ethics Board
Jennifer Wirawan, Investigator

WHISTLEBLOWER INVESTIGATION REPORT

Assertions and Results

In March 2016, our Office received a whistleblower complaint asserting seven Department of Health (Department) employees (Subjects JT, AF, MM, TG, GP, JB and LM), violated state contracting laws when they:

- Allowed purchase orders to be issued non-competitively and above the direct buy limit without sole source justification.
- Unbundled purchase orders to bypass the direct buy limit.
- Failed to use the competitive solicitation or sole source process for contracts.
- Failed to effectively manage existing contracts.
- Allowed contracts that violated state policies.

We reviewed five acquisitions (referenced below as Acquisitions One through Five) and determined whether the individual subjects were involved.

We found reasonable cause to believe:

- Subject MM failed to comply with state law when he approved the use of improper sole source exemptions and signed contracts awarded non-competitively in violation of state policies.
- Subject TG failed to comply with state law when she made purchases non-competitively and above the direct buy limit without proper sole source approval.
- Subject LM failed to comply with state law when he authorized the issuance of a contract that was awarded non-competitively and in violation of state policies.

We found no reasonable cause to believe Subjects JT, AF, GP and JB violated state law.

Background

State procurement laws are consolidated under the Department of Enterprise Services (DES), which has the authority to establish policies for the procurement of goods and services by all state agencies.

State law (RCW 39.26.120) requires agencies to competitively bid all purchases or contracts with few exceptions, including:

- Sole source contracts that comply with RCW 39.26.140
- Direct buy purchases

"Sole source" means a contractor providing goods or services of such a unique nature or sole availability at the location required that the contractor is clearly and

justifiably the only practicable source to provide the goods or services (RCW 39.26.010(23)).

According to state law (RCW 39.26.140) and DES policy (DES-140-00), unless otherwise exempt, all sole source contracts must:

- Be submitted to DES with supporting justification, and be made available for public inspection, no less than 10 working days before the start date of the contract.
- Be posted to DES' bid notification system for at least five working days. The policy requires that vendors "be given notice and an opportunity to demonstrate that a sole source contract is not justified."
- Be approved by DES before the contract becomes binding and services are performed.

There are 20 exemptions from the sole source policy. This report focuses on two: 1) Contracts where the vendor is specifically required by grant or legislation and 2) Software maintenance and support services when procured from the proprietary owner of the software.

A "direct buy" is a purchase made without using the competitive bid process. According to DES policy (DES-125-03), agencies are authorized to purchase goods and services up to $10,000, or $13,000 if the purchase is made from a microbusiness, minibusiness or small business. According to the policy, "Agencies may not unbundle or manipulate a purchase to have the purchase qualify as a direct buy procurement to avoid using a competitive process." Purchases exceeding the direct buy limit must be competitively bid. There are no exemptions from this policy.

Acquisitions 1 through 4

Laws and policies

Sole source reporting policy exemption four exempts from the sole source reporting policy "Software maintenance and support services when procured from the proprietary owner of the software. The procurement of software maintenance and support from third party vendors is not exempt from this policy."

According to DES's enterprise procurement policy manager, exemption four is for the purchase of software maintenance *if* the software program is already installed on the Department's computers. This exemption does not apply to initial purchases or subscriptions to software, even if that purchase includes maintenance and support.

Additionally, state law (RCW 43.105.054) and DES policies require IT-related contracts to meet the policies and standards of the Office of the Chief Information Officer (OCIO).

We spoke with an OCIO senior program manager who said that before entering into an IT contract, state agencies must conduct a risk assessment to determine the IT Investment oversight level (1, 2

or 3). Any project assessed at a level 2 or 3 is considered a major IT project and requires a concept review to be conducted by OCIO. Additionally, OCIO policy 141.10 1.2.1(3) states:

> The agency must request a security design review for maintenance and new development of systems and infrastructure projects when one or more of the following conditions exist:
>
> (3) An agency project or initiative impacts risk to state IT assets outside the agency.

To maintain system security, data integrity and confidentiality, OCIO policy 141.10 requires state agencies to "Include appropriate language in vendor contracts to require compliance with OCIO and agency security policies, standards, and requirements."

Acquisitions 1 and 2

The Department's Office of Community Health Systems (Program) operates two data collection systems to collect information on seriously injured patients in Washington. The information is used for data reporting and analysis for the prevention of trauma and the increase of trauma survival rates. A state rule (WAC 246-976-430) requires all designated trauma facilities, and all verified ambulance and aid services that transport trauma patients, to submit data to the Department. The submitted data contains protected health information, such as patient name, date of birth, social security number, patient ID number and diagnostic information.

Hospitals report data directly to the Department using a software program owned by Digital Innovations Corporation (DiCorp). The software is an "on-site system," which stores the data on Department servers. The Washington Emergency Medical Service Information System (WEMSIS), operated by ImageTrend, is a voluntary online reporting system used by emergency services to report pre-hospital emergency data to the Department. The WEMSIS program and submitted data are stored on ImageTrend servers.

After the expiration of the contracts with DiCorp and ImageTrend, 2004 and 2011, respectively, Department staff issued yearly purchase orders to both vendors, citing sole source exemption four. These purchases included licensing and hosting services, which, according to the statewide procurement policy manager for DES, are not considered maintenance and support.

We reviewed purchase orders for DiCorp and ImageTrend issued through June 2016. The purchase orders contained very little language regarding terms, security protections or a statement of work. None of the purchase orders contained the OCIO's required security language.

In January 2016, a Department IT technician sent a large file, via secure file transfer, containing protected health information to DiCorp so the company could correct an error it made when it deleted a file from Department servers. The IT technician requested that DiCorp staff delete the

encrypted and unencrypted versions once the file is no longer needed. DiCorp's emailed response that the files had been deleted was sent to the Department's Chief Information Security Officer (CISO).

The CISO responded to the email stating that even though DiCorp had a remote access agreement with terms and conditions for accessing data stored on the Department's servers, there was no agreement in place regarding data sent to and stored by DiCorp. She also noted that there was no current contract with DiCorp, only a purchase order, which "does not carry any liability protections for the agency," and that "DiCorp should not be able to even view the data without first having a clear contractual agreement in place."

We spoke with the CISO, who said that during an audit she found there was no OCIO security design review for ImageTrend's systems. She said she tried repeatedly for nearly two years to get information from ImageTrend in order to request a security design review, but ImageTrend did not respond to her requests.

The CISO reached out to the contract office for assistance with creating a more robust contract for DiCorp, and an amendment extending ImageTrend's prior contract. From February through April 2016, multiple discussions transpired between the CISO, contracts staff and Subject LM, who was the Program's deputy director. Discussions included what language each vendor would accept in the contracts, and whether the contracts should be competitively bid or sent to DES for approval as sole source contracts.

On February 16, 2016, Subject LM sent an email to his supervisor, advising the he had researched the DES policies and based on exemption four, "[b]oth Digital Innovations and ImageTrend are proprietary owners of the software and therefore we could do a purchase order without DES approval."

According to witnesses, Subject LM put pressure on the contracts specialist, the CISO, and other Department staff to complete the acquisitions quickly. He sent emails to staff with comments such as "We have approval from [Department] upper management to continue using purchase orders. This cannot be delayed by anyone;" "If our goal is to get this completed, I'm not sure we can asking [sic] for this change. We can discuss Thursday but this has to be signed soon and I think our risk is minimal;" and "I think our risk with DiCorp is minor and I agree the more we push the more issues will come up!"

In an email to the contract specialist dated April 12, 2016, Subject LM said, "We just need to complete this contract even though the details are not ideal." He added that he wanted the contract sent to DiCorp for signature as soon as possible.

We interviewed the contract specialist who said both contracts should have been competitively bid. She said she repeatedly expressed concerns that the contracts may violate state laws and policies to Subject LM and Subject MM (who worked in the Department's contracts and procurement office), but was instructed to proceed as directed. In one email, the contract specialist's supervisor wrote that the Program "has determined that the risks which you have identified below do not outweigh the potential benefit/consequences of moving forward" with the contracts.

The contract specialist provided Subjects LM and MM, and other Department staff, with a risk consultation regarding DiCorp in which she concluded that "[The Department] is required to compete this contract or justify it as a sole source and file a contract (not a [purchase order]) with DES for approval." She explained that sole source exemption four did not apply and said the contract lacked legal protections regarding: intellectual property infringement, rights in data, public disclosure of vendor proprietary information, compliance with state records retention schedules and access to data.

On April 21, 2016, the contract specialist emailed Subject LM twice to inform him that she was not going to endorse the DiCorp contract as it was not competitively bid according to law. Subject LM responded that he expected Subject MM to sign it.

The CISO sent two emails to Subjects LM and MM, advising them to "keep in mind that if the document is pulled for an OCIO compliance audit, it will be reported as a non-compliant finding."

Subject JT, who is in Subject MM's reporting structure, was consulted because the CISO was concerned that the security language in the DiCorp contract was not appropriate. In an interview, Subject JT said she advised Subject MM that if the contract specialist and the CISO approved the DiCorp contract and the CISO was "comfortable" with the security provisions, he could sign it.

Although Subject LM was aware, the CISO was concerned that the contract would not pass an OCIO audit, and the contract specialist had refused to endorse the document, he instructed a staff member to place a note on the internal procurement request indicating the contract was reviewed by the contract specialist and the CISO. Subject LM told us he gave this instruction because Subject MM said he would not sign the contract without their approval.

On May 5, 2016, Subject MM signed the contract, which was not compliant with OCIO standards. The following day procurement supervisor Subject TG, signed a $42,000 purchase order for a one-year subscription for DiCorp's program. Subject TG cited sole source policy exemption three, which is related to equipment, not software. During an interview, Subject TG said that was a typo as her intention was to use exemption four, "Software maintenance and support services when procured from the proprietary owner of the software." The purchase order incorporates the contract with DiCorp.

The amendment to the ImageTrend contract was signed on May 27, 2016, and included confidentiality provisions, data storage requirements and security terms. The Department did not complete a security design review of ImageTrend's systems, as required by OCIO policy.

Subjects LM and MM each asserted the other was responsible for the DiCorp contract. Subject LM told us he did not have authority over contracts, and he "did not violate any contracting laws since [he] did not sign the final documents." Subject MM said his signature allows the processing of the contract, the decision to issue the contract is up to the Program, under the direction of Subject LM.

We found reasonable cause to believe Subject LM, Subject MM, and Subject TG engaged in improper governmental actions when they allowed the issuance of purchase orders and contracts in violation of state procurement laws and policies.

Acquisition 3

In June 2014, the Department's Environmental Public Health Division (Division) entered into a contract with Ricoh, a digital business services company, to purchase document management software. Ricoh was required to export data from the Division's prior document management software (Oracle) to Ricoh's software.

About 15 months after entering into the contract, Ricoh disclosed that it did not have the capability to transfer the data. Ricoh stopped work while Division staff searched for a solution.

On October 15, 2015, Division staff contacted another vendor (ImageSource) to acquire the use of its mass export tool. On October 22, 2015, ImageSource informed Division staff that it did "not have a current contract" with the Department.

Division staff emailed a Department contract specialist for advice on the proper procedure for procuring the software. The contract specialist responded, "If it does not qualify as a direct buy you will either have to go out for competition or justify it as a sole source." She also advised, "The above processes take time so it is best to get moving."

On November 19, 2015, ImageSource emailed a quote for services above the direct buy limit. A Department IT manager emailed the quote to the contract specialist, and stated that Division management would like to "go through the 3 day" process to acquire the services. The contract specialist responded that it was not a three-day process, and asked if ImageSource was the only company able to provide this service. The IT manager responded that ImageSource and Oracle were the only vendors they knew had the tool.

Throughout December, Division staff and the contract specialist prepared the required documents to submit for DES approval of a sole source contract with ImageSource. Shortly after the documents were prepared and sent to the contract office for final review, Subject JB, a fiscal and

budgeting specialist, emailed Subject TG asking if there was a way to get the purchase through procurement instead of contracts.

During an interview, Subject JB said Subject TG advised that they could put it through procurement, and Subject MM agreed. Subject MM sent an email to Subject JB instructing her to follow Subject TG's direction and send it to procurement. He added that Subject TG "mentioned that someone in your area or formerly in your area can vouch for the sole source nature" and that it "make [sic] sense to go through [Subject TG's] Procurement team."

On December 23, Subject TG signed a purchase order for approximately $24,000 for the software program, which exceeded the $10,000 direct buy limit. On the purchase order, Subject TG cited sole source policy DES-140-00(9) exemption four, "Software maintenance and support services when procured from the proprietary owner of the software."

During an interview, Subject MM said that he did not remember why he authorized a purchase order with a sole source exemption. He said he does not believe the purchase qualified for exemption four. Subject TG said she believed the purchase did qualify for a sole source exemption.

We found Subject TG and Subject MM bypassed the competitive bid process and used an improper exemption to circumvent the reporting requirements of the sole source policy. Therefore, we found reasonable cause to believe an improper governmental action occurred.

Acquisition 4

In late 2013, the Department's Division of Information Resource Management (DIRM) began the process of selecting requirements management software. Over the next few months, DIRM staff reviewed options, developed a list of requirements, and attended demonstrations to determine which company's software best fit their needs; six were identified.

In April 2014, DIRM staff selected a vendor (Jama) to provide the software, and contacted the contracts and procurement office to complete the purchase. A Department manager informed staff they would most likely need to go through a public competitive bid process before they could contract with Jama. In response, Subject TG suggested staff start with a "request for information" to see how many vendors could provide the service. DIRM staff responded that they had the necessary information and knew which vendor they wanted.

The following month a representative from a competing company sent emails to DIRM staff describing the benefits of its software compared to Jama, and asked if there would be a competitive process. DIRM staff responded that they had not decided whether to do a competitive process. In June, representatives of the competing company again asked if there would be a competitive process; DIRM staff did not respond.

On July 7, 2014, one of Subject TG's staff signed a $53,000 purchase order for Jama's software, citing sole source exemption four, "Software maintenance and support services when procured from the proprietary owner of the software."

As Jama began implementation, the CISO became concerned with the lack of a formal contract and inadequate security controls present in the purchase order. She requested more information from Jama regarding its security controls and its license agreements. On August 5, 2014, the CISO sent additional security language to Subject TG for an addendum to the purchase order. The next day Subject TG signed an amended purchase order that included the security language.

On November 19, 2014, the CISO discovered Jama had not conducted an internal audit of its security practices, as required in the security amendment. The CISO drafted updated terms for another purchase order amendment, which was signed by procurement staff on December 1, 2014. As a result of these delays, DIRM was not able to begin using the software until January 2015, six months after the initial purchase order.

In November 2015, at the request of DIRM staff, Jama sent a renewal quote for a one-year subscription, licenses and hosting services. On November 17, 2015, Subject TG signed Jama's renewal quote and order form, and one of Subject TG's staff signed a purchase order for $27,380.

During an interview, Subject TG said that after DIRM staff explained why they chose Jama she decided to issue a purchase order using a sole source reporting exemption. She was aware there were at least five other vendors who could provide the requirements management software. She said she stands by her decision to use the exemption.

Both the 2014 and the 2015 purchase orders were over the direct buy limit, and were not competitively bid. Because there were at least five vendors who provided the same or similar services as Jama's software, these purchases should have been competitively bid or submitted to DES for sole source approval.

We found Subject TG failed to competitively bid the Jama acquisition and used an improper exemption to circumvent the reporting requirements of the sole source policy. Therefore, we found reasonable cause to believe an improper governmental action occurred.

Acquisition 5

This section focuses on sole source reporting policy exemption five, which exempts from the policy "Contracts where the vendor is specifically required by a grant or legislation."

The Washington Tracking Network (WTN) is a website created to help residents find health information regarding their communities and surrounding areas. Development of the WTN began in 2011 and is expected to be completed by 2019.

The Department received federal grants to create and operate the WTN.

In February 2013, Subject GP, a manager in the Department's Office of Environmental Public Health Sciences, applied for a federal grant for the WTN project. In the grant application, Subject GP listed contractor Durkin and Associates (Durkin) as a sole source provider to "improve the performance, function, scalability and sustainability" of the current project database. Subject GP wrote in the application that Durkin is "uniquely qualified" to work on this project due to a past and ongoing relationship with the Department.

While Subject GP identified Durkin as a sole source provider of the required services, Department staff had not completed any of the DES filing requirements for sole source approval. In addition, Department staff had not posted notice of the intended sole source contract on the DES bid notification system.

In July 2013, the Department entered into a $100,000 contract with Durkin using sole source exemption five, for "Contracts where the vendor is specifically required by a grant or legislation." The performance period for this contract was July 1, 2013 through February 28, 2014. In 2014, the Department and Durkin entered into another contract for $185,000 to continue work on the WTN. The performance period for this contract was September 1, 2014 through July 31, 2015.

We spoke with witnesses who said naming vendors in grant applications to bypass the competitive bid process was a prior practice at the Department. They said it was believed to be appropriate at one time, but the Department has since stopped this practice.

During an interview, Subject GP said he was following the Department's past practice and his understanding of competitive contracting exceptions. He said he named Durkin in his grant application because of their unique past experience working on the Department's data security model, which was directly applicable to the proposed contract work. He added that the newest WTN contract has undergone a competitive bid process at the direction of executive management, Subjects AF and JT. Because the asserted improper action occurred in 2013 and the practice of naming vendors in grant applications to bypass the competitive process is no longer followed, we did not investigate further.

Regarding the assertion that purchases were unbundled to bypass the direct buy limit, we found two purchase orders were issued for additional work on the WTN. On October 9, 2015, Subject

TG signed a $7,295 purchase order for 60 hours of emergency IT support services to allow Durkin to fix problems with the WTN. In April 2016, a purchase order for $8,680 was signed for an additional 60 hours of maintenance of the WTN. We reviewed the purchase orders and related emails, and found no evidence these transactions were associated and unbundled to remain below the direct buy limit.

Therefore, we found no reasonable cause to believe an improper governmental action occurred related to acquisition five.

Department's Plan of Resolution

The Department of Health thanks the Auditor's Office for the opportunity to respond to this Whistleblower report. We take allegations of wrongdoing seriously and appreciate the investigators' work and final recommendations.

We would like to take this opportunity to delineate why the Department chose the courses of actions described in this report and acknowledge the areas we need to improve.

Acquisitions 1 and 2

One of the Department's critical public health missions is the operation of the Trauma Registries (a hospital and an emergency medical services registry). To support these registries, the Department uses two data collection systems. One created by TriAnalytics and the other by ImageTrend.

It is Program's understanding that years ago a formal selection process was performed and TriAnalytics was the vendor chosen. The rights to this software were later purchased around 1996 or 1997 by Digital Innovations (DiCorp), a company created by the former lead programmer for TriAnalytics.

A formal selection process was performed to select the other data collection system. ImageTrend was the successful bidder.

The Department's ongoing relationship with each of these entities is one of annual maintenance and support which is necessary to keep the two collection systems working.

The Department pays DiCorp $42,000 annually. The purpose of this payment, as described in the July 1, 2016 agreement between the Department and DiCorp states, "The current rate of maintenance for the licensee is $42,000." This maintenance, which was purchased through the proprietary owner, is an allowable exemption under Sole Source Contract's Policy #DES-140-00 section nine, exemption four.

For the period July 1, 2016 – June 30, 2017 the Department signed an agreement with ImageTrend to pay approximately $115,000. Of this $115,000, approximately $110,000 is for annual support

and hosting. We agree exemption four does not include hosting costs. However, we pay hosting costs to ImageTrend, the successful bidder of a contract that was competitively bid over ten years ago, because the software is located on their servers. In this scenario, the Department is using section nine, exemption four to ensure the Department receives continued support needed from the proprietary owner of this software. The report states that "According to DES's enterprise procurement policy manager, exemption four is for the purchase of software maintenance if the software program is already installed on the Department's computers." Our concern is that this is only an interpretation. The actual policy does not state the software must already be installed on Department computers. Additionally, we were operating under DES guidance that indicated exemptions are written at a high level so customers are not boxed in.

We appreciate the auditor's noted concerns regarding OCIO standards. To ensure compliance with OCIO Standard 141.10, Securing Information Technology Assets, the Department and DiCorp signed a contract amendment that updated information security language on November 10, 2016. The Department is scheduled to complete an IT risk assessment of ImageTrend's WEMSIS in March, 2017. Based on the risk assessment results, the Department will assess and address any issues identified and may consult with the Office of Cyber Security to determine whether a design review is recommended (IAW OCIO 141.10, para 1.2.1 Design Review).

Acquisition 3

The Department acknowledges ImageSource should not have been deemed a contract exempt from sole source contracting. However, the Department did not avoid competition because there were two appropriate routes the Department could have taken:

- *The original contract was with Ricoh, which is a DES Master Contracted vendor. Approximately fifteen months after the contract was signed Ricoh found they could not provide the needed service. This could have been satisfied by Ricoh obtaining a subcontractor. A DES Master Contracted vendor is not required by DES to competitively bid for a subcontractor.*

- *By the time Ricoh disclosed that it did not have the capability to perform the service, time was running very short and due to the nature of the work needing to be done an emergency contract could have been let. The decision to execute an emergency contract rests solely with agencies.*

In future like situations, the Department will ensure one of the above routes are used.

Acquisition 4

The Department acknowledges the initial acquisition of the requirements management software (Jama) should have been competitively bid or submitted to DES for sole source approval. We will reach out to DES for guidance as how to move forward when the vendor business model is in one-year subscription increments.

State Auditor's Office Concluding Remarks

We thank Department officials and personnel for their assistance and cooperation during the investigation.

We will follow-up with the Department to determine whether appropriate action has been taken, as we are charged to do under state law. If appropriate action has not been taken, the auditor will report the determination to the governor and to the legislature and may include this determination in the next agency audit.

WHISTLEBLOWER INVESTIGATION CRITERIA

We came to our determination in this investigation by evaluating the facts against the criteria below:

RCW 39.26.120 - Competitive solicitation.

> (1) Insofar as practicable, all purchases of or contracts for goods and services must be based on a competitive solicitation process. This process may include electronic or web-based solicitations, bids, and signatures. This requirement also applies to procurement of goods and services executed by agencies under delegated authority granted in accordance with RCW 39.26.090 or under RCW 28B.10.029.
>
> (2) Subsection (1) of this section applies to contract amendments that substantially change the scope of work of the original contract or substantially increase the value of the original contract.

RCW 39.26.125 - Competitive solicitation—Exceptions, states in part:

> All contracts must be entered into pursuant to competitive solicitation, except for:
>
> > (2) Sole source contracts that comply with the provisions of RCW 39.26.140;
> >
> > (3) Direct buy purchases, as designated by the director. The director shall establish policies to define criteria for direct buy purchases. These criteria may be adjusted to accommodate special market conditions and to promote market diversity for the benefit of the citizens of the state of Washington;

Department of Enterprise Services Policy #DES-125-03 Direct Buy Purchase/Procurements

> 3) Direct Buy Purchase Authorization:
>
> > Effective January 1, 2013, agencies are authorized to purchase goods and services up to a cost of $10,000 (excluding sales tax) directly from a vendor and without competition. In addition, agencies are authorized to purchase goods and services up to a cost of $13,000 (excluding sales tax) directly from a vendor and without competition if the purchase is being made from a microbusiness,

minibusiness, or small business as those terms are defined by RCW 39.26.010 (19), (20) and (21).

4) Additional Requirements:

1) Agencies must use existing "qualified master contracts" before engaging in a direct buy. Only when an existing qualified master contract cannot justifiably satisfy agency needs may the agency make a direct buy purchase.

2) Agencies are encouraged to buy from in-state small businesses to include certified minority, women and veteran owned businesses.

3) Unless otherwise exempt, procurements that exceed the direct buy limit must be competitively awarded, unless otherwise exempt from competition.

4) Agencies may not unbundle or manipulate a purchase to have the purchase qualify as a direct buy procurement to avoid using a competitive process.

RCW 39.26.140 - Sole source contracts, states in part:

(1) Agencies must submit sole source contracts to the department and make the contracts available for public inspection not less than ten working days before the proposed starting date of the contract. Agencies must provide documented justification for sole source contracts to the department when the contract is submitted, and must include evidence that the agency posted the contract opportunity at a minimum on the state's enterprise vendor registration and bid notification system.

(2) The department must approve sole source contracts before any such contract becomes binding and before any services may be performed or goods provided under the contract. These requirements shall also apply to all sole source contracts except as otherwise exempted by the director.

(3) The director may provide an agency an exemption from the requirements of this section for a contract or contracts. Requests for exemptions must be submitted to the director in writing.

Department of Enterprise Services Policy #DES-140-00 Sole Source Contracts

Effective January 1, 2013 and unless otherwise exempt, all agency sole source contracts must:

1) Be submitted to DES, with supporting justification, not less than 10 working days prior to the contract start date.

2) Be approved by DES before the contract becomes binding, services are performed and goods are received.

3) Be made available for public inspection not less than 10 working days prior to the contract start date.

In addition, notice of all agency sole source contract opportunities must be posted on the state's enterprise vendor registration and bid notification system (currently the Washington Electronic Business Solution (WEBS)) for at least five (5) working days.

The following types of contracts are exempt from this Sole Source Contracts policy:

3) Original equipment manufacturer (OEM) maintenance service contracts and parts purchases when procured directly from the OEM.

4) Software maintenance and support services when procured from the proprietary owner of the software. The procurement of software maintenance and support from third party vendors is not exempt from this policy.

5) Contracts where the vendor is specifically required by a grant or legislation.

RCW 39.26.150 - Public notice—Posting on enterprise vendor registration and bid notification system.

(1) Agencies must provide public notice for all competitive solicitations. Agencies must post all contract opportunities on the state's enterprise vendor registration and bid notification system. In addition, agencies may notify contractors and potential bidders by sending notices by mail, electronic transmission, newspaper advertisements, or other means as may be appropriate.

(2) Agencies should try to anticipate changes in a requirement before the bid submittal date and to provide reasonable notice to all prospective bidders of any resulting modification or cancellation. If, in the opinion of the agency, it is not possible to provide reasonable notice, the submittal date for receipt of bids may be postponed and all bidders notified.

RCW 39.26.180 - Contract management, states in part:

(1) The department must adopt uniform policies and procedures for the effective and efficient management of contracts by all state agencies. The policies and procedures must, at a minimum, include:

(a) Precontract procedures for selecting potential contractors based on their qualifications and ability to perform;

(b) Model complaint and protest procedures;

(c) Alternative dispute resolution processes;

(d) Incorporation of performance measures and measurable benchmarks in contracts;

(e) Model contract terms to ensure contract performance and compliance with state and federal standards;

(f) Executing contracts using electronic signatures;

(g) Criteria for contract amendments;

(h) Post contract procedures;

(i) Procedures and criteria for terminating contracts for cause or otherwise; and

(j) Any other subject related to effective and efficient contract management.

(2) An agency may not enter into a contract under which the contractor could charge additional costs to the agency, the department, the joint legislative audit and review committee, or the state auditor for access to data generated under the contract. A contractor under such a contract must provide access to data generated under the contract to the contracting agency, the joint legislative audit and review committee, and the state auditor.

(3) To the extent practicable, agencies should enter into performance-based contracts. Performance-based contracts identify expected deliverables and performance measures or outcomes. Performance-based contracts also use appropriate techniques, which may include but are not limited to, either consequences or incentives or both to ensure that agreed upon value to the state is received. Payment for goods and services under performance-based contracts should be contingent on the contractor achieving performance outcomes.

RCW 43.105.054 Governing information technology—Standards and policies—Powers and duties of office, states in part:

(1) The director shall establish standards and policies to govern information technology in the state of Washington.

(2) The office shall have the following powers and duties related to information services:

(a) To develop statewide standards and policies governing the:

(i) Acquisition of equipment, software, and technology-related services;

(ii) Disposition of equipment;

(iii) Licensing of the radio spectrum by or on behalf of state agencies; and

(iv) Confidentiality of computerized data;

RCW 43.105.215 Security standards and policies—State agencies' information technology security programs, states in part:

(2) Each state agency information technology security program must adhere to the office's security standards and policies.