ITPS WORK REQUEST #24-01

NOVEMBER 6, 2023

2nd Tier Solicitation

Under Master Contract No. 08215

Category 10: Infrastructure Services

For IT Security Reviews and Cybersecurity Consulting

INTRODUCTION

The Washington State Investment Board (WSIB) is issuing this 2nd Tier solicitation under Master Contract, 08215. **Only Bidders awarded a Tier 1 Master Contract for Category 10: Infrastructure Services can bid on this opportunity.**

BACKGROUND

The WSIB is a public agency of the State of Washington established to administer the state's investment activity. The WSIB investment programs include both qualified (IRC § 401(a)) retirement programs and non-qualified programs. To learn more about the WSIB, please visit our website at www.sib.wa.gov.

Pursuant to Chapter 39.26 of the Revised Code of Washington (RCW), the WSIB is issuing this IT Professional Services (ITPS) Work Request to contract with a firm(s) to provide A) IT security reviews five WSIB external real estate investment managers' ("Intermediaries'") IT security policies and practices, and B) ongoing cybersecurity consulting services.

SCOPE OF WORK

The contractor will work with appropriate WSIB and Intermediary staff, and (where applicable) third-party IT security service providers to review systems and documentation to accomplish the objectives outlined below:

A. Category A Services – Intermediary Operational Due Diligence (ODD) IT Security Reviews

1) Contractor will conduct comprehensive ODD IT security reviews of five WSIB Intermediaries' IT security policies and practices. To accomplish this, for each review the contractor will:
   a. Assess compliance with the applicable sections of the WSIB Recommended Real Estate Intermediary Control Guidelines (see Attachment A) related to IT security.
   b. As applicable, evaluate the adequacy of procurement and monitoring activities of the Intermediary's third-party IT service provider(s).
   c. Assess the centralized policies and procedures the Intermediary has in place designed to oversee/monitor the IT security of its investments in underlying real estate operating companies (REOCs), to include cybersecurity incident reporting.
   d. Compare the Intermediary's IT security policies and practices with current industry standards and best practices, given the size and structure of the organization, identifying gaps.
   e. Report results, assess any identified risks, and make recommendations for improvement.
   f. At the WSIB's request, be available to attend exit calls with Intermediaries at the conclusion of each review to present results and/or answer questions regarding work performed.
   g. At the WSIB's request, follow up on remediation efforts for identified issues.
2) Summary Report: At the conclusion of all five Intermediary reviews, the contractor will produce and present a comprehensive report that includes, at a minimum, the following:
   a. A summary of all of the five Intermediaries' IT security/cybersecurity practices at the portfolio level, control gaps, associated risk ratings, and recommendations for improvement.
   b. An assessment of the WSIB incident reporting procedure, as it relates to cybersecurity events, and suggested improvements.
   c. Future review/testing strategy recommendations, based on risk, for the WSIB to consider incorporating into periodic ODD reviews based on best practices.
3) Strategic Project: Contractor will participate in a strategic project to update the WSIB Real Estate ODD Program as it relates to IT security/cybersecurity. The small group project will consider overall program

requirements, as well as WSIB Recommended Real Estate Intermediary Control Guidelines, based on feedback, experience, and industry best practices.

B. Category B Services – Cybersecurity Consulting

Assist the WSIB on an as-needed basis by providing cybersecurity consulting services related to the Intermediaries.

This Solicitation is divided into six (6) sections:

- Section 1 provides a summary table of relevant deadlines for responding to the Solicitation and identifies contact information for the WSIB Procurement Coordinator.
- Section 2 provides important information about the procurement that is designed to help interested bidders evaluate the potential opportunity, including the purpose of the procurement, information about the resulting Contract, and the performance requirements.
- Section 3 identifies how the WSIB will evaluate the bids.
- Section 4 identifies how to prepare and submit a bid for this ITPS Work Request, including detailed instructions regarding what to submit and how to submit your bid.
- Section 5 details the applicable requirements to file a complaint, request a debrief conference, or file a protest regarding this ITPS Work Request.
- Section 6 provides information pertaining to doing business with the State of Washington, including the WSIB's efforts to enable Washington's small and diverse businesses to compete for and participate in state procurements.

In addition, this Solicitation includes the following Exhibits:

- *Exhibit A – Required Bidder Information*: These exhibits identify information that bidders must provide to constitute a responsive bid. Also see Section 4, below.
- Exhibit A-1 – Bidder's Certification
- Exhibit A-2 – Bidder's Profile and References
- *Exhibit B – Questionnaire*: This exhibit contains the questions bidders must respond to which will be evaluated by the WSIB.
- *Exhibit C – Fee Schedule*: This exhibit provides the pricing format bidders will complete as part of their bid.
- *Exhibit D – Work Order #24-01*: This exhibit is a draft of the Contract that any successful bidder will execute. If there are business concerns or other issues with the terms and conditions in this exhibit, provide proposed changes within the form. Note, however, that the WSIB reserves the right to approve or disapprove proposed changes and to take contract modifications under consideration during the evaluation process.

SECTION 1 – DEADLINES, QUESTIONS, PROCUREMENT COORDINATOR, AND MODIFICATION

This section identifies important deadlines for this ITPS Work Request, where to direct questions regarding the Competitive Solicitation, and the process for potential amendments or modifications.

1.1. **SOLICITATION SCHEDULE**. The following table identifies important dates for this ITPS Work Request:

ITPS WORK REQUEST SCHEDULE	
ITEM	**DATE**
Competitive Solicitation Posting Date	November 6, 2023
Bidder Questions Due to the WSIB	November 20, 2023
WSIB Answers to Questions Posted	November 29, 2023
Deadline for Submitting Bids	December 8, 2023
Anticipated Announcement of Apparent Successful Bidder(s)	January 26, 2024
Contract Negotiation	January 29 - February 16, 2024
Anticipated Contract(s) Start Date	March 1, 2024

1.2. **PROCUREMENT COORDINATOR.** During the ITPS Work Request process, all bidder communications must be directed to the Procurement Coordinator listed in the table below. Unauthorized bidder contact regarding this Solicitation with other state employees involved with this process may result in bidder disqualification.

PROCUREMENT COORDINATOR	
Name	Isaac Williamson
Telephone	(360) 956-4604
Email	contracts@sib.wa.gov
Subject Line	ITPS Work Request #24-01

1.3. **ITPS WORK REQUEST QUESTIONS**. Questions or concerns regarding this ITPS Work Request will be addressed consistent with the above schedule. The WSIB will provide written answers for questions received which will be posted to Washington's Electronic Business Solution (WEBS).

a. Bidders are encouraged to make any inquiries regarding this Solicitation as early in the process as possible. If a bidder does not notify the WSIB of an issue, exception, addition, or omission, the WSIB may consider the matter waived by the bidder for protest purposes.

b. If bidder inquiries result in changes to the Solicitation, written amendments, which may include the WSIB answers to bidder questions, will be issued and posted on WEBS. In no event will oral communications regarding the Solicitation be binding.

1.4. **SOLICITATION MODIFICATION**. The WSIB reserves the right to amend and modify this Solicitation. Notifications of amendments and other correspondence pertinent to this Solicitation will be posted in the Washington Electronic Business Solution WEBS.

SECTION 2 – CONTRACT, PERIOD OF PERFORMANCE, PLACE OF PERFORMANCE, PERFORMANCE REQUIREMENTS

2.1. **CONTRACT**. The form of the Contract that will be awarded is attached as ***Exhibit D –*** *Work Order #24-01*.

2.2. **PERIOD OF PERFORMANCE**. The WSIB anticipates Category A work will take place between March 1, 2024, and December 31, 2025, Category B services will begin March 1, 2024, through February 28, 2029. The period of performance for Category B services may be extended for up to an additional five years through mutual agreement of the parties.

2.3. **PLACE OF PERFORMANCE.** For Category A Intermediary ODD IT Security Reviews, bidders should propose two separate ODD bids in their response:

a. ODD IT Security Reviews with on-site visit. (The WSIB anticipated the on-site work will be conducted at the Intermediaries' headquarters location as listed in the table in Section 2.4 below).

b. ODD IT Security Reviews without on-site visit.

If the Contractor is unwilling or unable to provide a bid for ODD with an on-site visit, the WSIB will still review the bid. As part of the response, the Contractor should identify any potential limitations and possible solutions to ensure the work can be conducted remotely.

For all other services in this request, the Contractor should plan to complete the work remotely.

2.4. **PERFORMANCE REQUIREMENTS**

A. Category A Services

1) **Intermediary ODD IT Security Reviews**

The WSIB conducts ODD reviews of its full governance real estate Intermediaries on a two-year rotation. The Intermediaries are small to medium-sized organizations with commensurate IT and cybersecurity resources dedicated to protecting the IT assets of the firms. Intermediary ODD review timing and high-level information follows:

Intermediary	Questionnaire/Doc Request	WSIB On-site Fieldwork	FTE	HQ Office
i.	May 2024	Jul 2024	28	Hong Kong
ii.	Aug 2024	Oct 2024	19	Chicago, IL
iii.	Jan 2025	Mar 2025	21	Amsterdam
iv.	May 2025	Jul 2025	51	Chicago, IL
v.	July 2023	Sept 2023	31	Chicago, IL

a. Intermediary Guideline Controls Reviewed. Following the timelines in the table above, the contractor will conduct comprehensive IT security reviews of five Intermediaries, evaluating existing Intermediary IT security policies, procedures, and controls to determine compliance with the *WSIB Recommended Real Estate Intermediary Control Guidelines* (see Attachment A).

   Expected work will include a questionnaire/documentation request process, review of documentation, inquiry of Intermediary and (as applicable) third-party IT managed service/managed security service provider staff, and testing of controls in place to support Contractor's assessment of compliance and to determine controls' effectiveness.

b. Intermediary Third-Party IT Service Provider Oversight. As applicable, the contractor will assess the Intermediary's practices for monitoring any third-party IT service providers, and/or IT security service providers focused on the security, confidentiality, and accessibility of Intermediary data; compare with best practices; and make improvement recommendations. This includes the processes, controls over, and practices related to:

   i. Initial vendor procurement reviews, including an assessment of the service provider's cybersecurity posture/associated risks.

   ii. Data sharing agreements and contract requirements.

   iii. Ongoing monitoring, including but not limited to, review of and follow up on required reporting (review of SOC reporting, implementation of controls at the user entities), and discussion with vendors.

   iv. Proper classification, storage, and handling of Intermediary data.

   v. Removal of data at the conclusion of the contract.

   vi. Insurance levels to protect the Intermediary in the event of cybersecurity or other incidents at the vendor.

c. Intermediary Oversight of Real Estate Operating Company (REOC) IT Security/Cybersecurity Controls and Practices. Contractor will review and evaluate the policies, procedures, and controls the Intermediary has in place designed to oversee/monitor the IT security practices of its investments in underlying REOCs. WSIB Intermediaries are responsible for proper oversight of those underlying platform entities, having controlling interests, and significant governance rights to do so. WSIB must have a high degree of assurance as to the strength of the Intermediary's governance structure with regard to IT security/cybersecurity.

   As background, the Intermediaries hire an outsourced internal audit service provider to review the respective controls of their underlying REOC investments on a two-year rotation, which includes in part, IT security/cybersecurity controls. Risks identified as moderate or high by the internal audit service provider are reported to the WSIB and monitored for resolution. In addition, some Intermediaries have also hired IT security/cybersecurity consultants to perform more detailed reviews of REOC IT security/cyber control practices on a different cadence.

   Through review of documentation (which may include Intermediary written guidance to REOCs, other ongoing monitoring, third-party reviewers' engagement letters, scopes of work, risk assessments, reporting, remediation of risks identified, and cybersecurity incident response documentation/reports), Contractor will assess the quality of the overall framework to ensure it is fit for purpose.

   In its assessment of the Intermediary's response and oversight of REOC cybersecurity incidents, Contractor will:

   i. Determine whether the Intermediary's written guidelines to their REOCs provide adequate instruction or guidance on how a REOC is to perform cybersecurity incident investigations.

Describe any guidance that should be included so that root cause can be fully explained, and future incidents prevented, detected and remediated in a timely manner.

ii. Consider the quality of the assurance providers, and thoroughness of the assurance reviews.

iii. Assess how proactively the Intermediary takes recommendations or issues raised during incidents and uses them to prevent or implement change across their other investment REOCs.

d. Compare Intermediary practices above with current industry standards (CIS or NIST) and best practices, given the size and structure of the organization, identifying gaps.

e. Following each Intermediary review, contractor will provide the following deliverables:

i. Presentation of preliminary results to WSIB and Intermediary staff prior to providing results in a report.

ii. Prepare a written report including an executive summary, summary of work performed by sections (a-d above), results obtained, an assessment of any identified gaps/issues/observations (non-trivial), and an identification of severity/risk rating, along with recommendations to address and/or improve. The report and recommendations should be written in such a way that an informed, non-IT professional can readily understand the concerns raised. WSIB and the Contractor will work together to ensure the final report and the executive summary meets the needs of both parties. Report will be delivered to the WSIB by agreed-upon due dates in concert with ODD reviews.

iii. At the WSIB's request, contractor will be available to attend exit calls with Intermediaries at the conclusion of each review to present results and/or answer questions regarding work performed.

iv. Follow up on remediation efforts for identified issues, if any; Contractor will be available to review corrective action when noted complete and report to WSIB.

2) **Comprehensive Summary Report on Intermediary IT Security Practices**

At the conclusion of all five Intermediary ODD reviews (estimated completion April 2025), contractor will prepare a written report including, at a minimum:

a. An executive summary, description of the work performed, results obtained, control gaps, associated risk ratings, and recommendations for improvement.

b. Assessment of the WSIB incident reporting procedure (as it relates to cybersecurity events) including recommended enhancements focused on root cause identification and corrective actions taken to reduce the likelihood of another incident.

c. Future review/testing strategy recommendations, based on risk, for the WSIB to consider incorporating into periodic ODD reviews based on best practices.

d. Present results to the WSIB, and be available to attend meetings virtually, as needed, for questions regarding the work performed.

3) **Participate in a Strategic Project to Update the WSIB Real Estate ODD Program as IT Security Consultant**

Contractor will participate in the next strategic project to update the WSIB Real Estate Operational Due Diligence Program as it relates to IT Security; the small project group will consider improvements to overall program requirements such as ODD rotation and REOC oversight, as well as WSIB Recommended Real Estate Intermediary Control Guidelines, based on feedback, experience and industry best practices. Work is expected to include input and review of updated guideline documentation, and participation in two to three virtual project meetings/calls.

B. Category B Services: Cybersecurity Consulting

Assist the WSIB on an as-needed basis by providing cybersecurity consulting services related to the Intermediaries. These services may include, but not be limited to, review of incident reports received, participation in virtual meetings to advise, remediation follow-up, guideline updates/reviews to identify potential gaps and improvements, etc.

SECTION 3 – BID EVALUATION

This section identifies how the WSIB will evaluate bids for this Competitive Solicitation.

3.1. **OVERVIEW**. The WSIB will evaluate bids for this Solicitation as described below.

- Bidder responsiveness, performance requirements, price factors, and responsibility, will be evaluated based on the process described herein.
- Any bidder whose bid is determined to be non-responsive will be rejected and will be notified of the reasons for this rejection.
- The WSIB reserves the right to: (1) Request clarification regarding any bid; (2) Waive any informality; (3) Reject any or all bids, or portions thereof; (4) Accept any portion of the bid unless the bidder stipulates all or nothing in their bid; (5) Cancel the Solicitation and, if desired, re-solicit bids; and/or (6) Negotiate with the lowest responsive and responsible bidder(s) to determine if such bid can be improved.
- The WSIB will use the following process and evaluation criteria for an award of the Contract:

EVALUATION PROCESS	
Criteria	Available Points
Responsiveness	Pass/Fail
Response to Questionnaire	300
Cost	200
Evaluation Point Total	500
Responsibility	Pass/Fail
Interviews (optional)	See 3.6

- WSIB reserves the right to modify the evaluation process and points as set forth in this section to ensure compliance with state law or policy.

3.2. **BID RESPONSIVENESS (STEP 1)**. Proposals will be reviewed initially to determine, on a pass/fail basis, whether they meet all administrative requirements specified herein.

3.3. **RESPONSE TO EXHIBIT B QUESTIONNAIRE (STEP 2)**. An evaluation team will evaluate bidder's response to Exhibit B – Questionnaire and award points consistent with their best professional judgment.

3.4. **BID PRICING EVALUATION (STEP 3)**. The WSIB will evaluate bids by comparing the bidder's qualifications and the reasonableness of the submitted bid prices as provided in *Exhibit C*. Each bidder will be awarded points accordingly.

3.5. **BIDDER RESPONSIBILITY ANALYSIS (STEP 4).** For responsive bids, the WSIB must determine whether the bidder is a 'responsible bidder.' Accordingly, the WSIB will make reasonable inquiry to determine bidder responsibility

on a pass/fail basis. In determining bidder responsibility, the WSIB will consider the following statutory (See RCW 39.26.160) elements:

- The bidder's ability, capacity, and skill to perform the contract or provide the service required.
- The bidder's character, integrity, reputation, judgment, experience, and efficiency.
- Whether the bidder can perform the contract within the time specified.
- The bidder's performance quality pertaining to previous contracts or services.
- The bidder's compliance with laws relating to the contract or services.
- Such other information as may be secured having a bearing on the decision to award the Contract.

In addition, the WSIB may consider the following:

- Financial Information: The WSIB may request financial statements, credit ratings, references, record of past performance, clarification of bidder's offer, on-site inspection of bidder's or subcontractor's facilities, or other information as necessary to determine bidder's capacity to perform and the enforceability of bidder's contractual commitments. Failure to respond to these requests may result in a bid being rejected as non-responsive.
- References: The WSIB reserves the right to use references to confirm satisfactory customer service, performance, satisfaction with service/product, knowledge of products/service/industry and timeliness. Any negative or unsatisfactory reference can be reason for rejecting a bidder as non-responsible.

3.6. **INTERVIEWS / ORAL EVALUATIONS (STEP 5 - OPTIONAL).** The WSIB may choose to conduct virtual interviews for the final selection of the Apparently Successful Bidder(s). The virtual interviews will be evaluated to develop a consensus decision of the evaluation team.

3.7. **CONTRACT NEGOTIATIONS (STEP 5)**. The WSIB may negotiate with the highest scored responsive, responsible bidder to finalize the Contract and to determine if the bid may be improved. If, after a reasonable period of time, the WSIB, in its sole judgement, cannot reach agreement on acceptable Contract terms with such bidder, the WSIB may suspend negotiations and undertake negotiations with the next highest scored responsive, responsible bidder as determined by the evaluations.

3.8. **ANNOUNCEMENT OF APPARENT SUCCESSFUL BIDDER**. The WSIB will determine the Apparent Successful Bidder ("ASB"). The ASB will be the responsive and responsible bidder(s) that best meet(s) the Solicitation requirements and presents the best total value.

- Designation as an ASB does not imply that the WSIB will issue an award for a Contract to your firm. Rather, this designation allows the WSIB to perform further analysis and ask for additional documentation. The bidder must not construe this as an award, impending award, attempt to negotiate, etc. If a bidder acts or fails to act as a result of this notification, it does so at its own risk and expense.
- Upon announcement of the ASB(s), bidders may request a debrief conference as specified in Section 5.

3.9. **AWARD OF CONTRACT**. Subject to protests, if any, the WSIB and the ASB(s) will enter into a Contract as set forth in ***Exhibit D – Work Order #24-01.*** The WSIB reserves the right to award on an all-or-nothing consolidated basis. Following the award of the Contract, all bidders registered in WEBS will receive a Notice of Award delivered to the bidder's email address provided in the bidder's profile in WEBS.

3.10. **BID INFORMATION AVAILABILITY**. Upon announcement of ASB(s), all bid submissions and all bid evaluations are subject to public disclosure pursuant to Washington's Public Records Act. *See* RCW 39.26.030(2).

SECTION 4 – HOW TO PREPARE AND SUBMIT A BID FOR THIS COMPETITIVE SOLICITATION

This section identifies how to prepare and submit your bid for this Competitive Solicitation. In addition, bidders will need to review and follow the Solicitation requirements including those set forth in the exhibits, which identifies the information that bidders must provide to constitute a responsive bid. By responding to this Solicitation and submitting a bid, bidders acknowledge having read and understood the entire Solicitation and accept all information contained within this Competitive Solicitation.

4.1. **BIDDER COMMUNICATIONS REGARDING THIS COMPETITIVE SOLICITATION**. During the Solicitation process, all bidder communications regarding this Solicitation must be directed to the Procurement Coordinator for this Competitive Solicitation. *See* Section 1.2 of this Competitive Solicitation. Bidders should rely only on this Solicitation and written amendments to the Solicitation issued by the Procurement Coordinator. In no event will oral communications regarding the Solicitation be binding.

- Bidders are encouraged to make any inquiry regarding the Solicitation as early in the process as possible to allow consideration and, if warranted, respond to the inquiry. If a bidder does not notify WSIB of an issue, exception, addition, or omission, WSIB may consider the matter waived by the bidder for protest purposes.
- If bidder inquiries result in changes to the Solicitation, written amendments will be issued and posted on WEBS.
- Unauthorized bidder contact regarding this Solicitation with other state employees involved with the Solicitation may result in bidder disqualification.

4.2. **PRICING**. Bid prices must include all cost components needed for the services as described in this Solicitation. As noted in **Exhibit C – Fee Schedule** bidders have the option to provide a flat fee where applicable. In addition to hourly rates bidders should provide a blended hourly rate which includes all travel related costs where applicable.

- Inclusive Pricing: Bidders must identify and include all cost elements in their pricing. In the event that bidder is awarded a Contract, the total price for the services shall be bidder's price as submitted. Except as may be provided in the Contract, there shall be no additional costs of any kind.
- Credit Cards (P-Cards): In the event that bidder is awarded a Contract, the total price for the services shall be the same regardless of whether Purchasers make payment by cash, credit card, or electronic payment. Bidder shall bear, in full, any processing or surcharge fees associated with the use of credit cards or electronic payment.

4.3. **BID SUBMITTAL CHECKLIST – REQUIRED BID SUBMITTALS**. This section identifies the bid submittals that must be provided to constitute a responsive bid. The submittals must be delivered as set forth below. Bids that do not include the submittals identified below may be rejected as nonresponsive. In addition, a bidder's failure to complete any submittal as instructed may result in the bid being rejected. Bidders may not provide unsolicited materials. For any supplemental materials expressly required by the WSIB in writing, bidders must identify such supplemental materials with the bidder's name.

☐ **EXHIBIT A-1 – BIDDER'S CERTIFICATION**

This document is the Bidder's Certification. Complete the certification, attach it to the bid along with any exceptions or required explanations, and submit it to the WSIB.
Note: The Certification must be complete. Where there are choices, bidder must check a box. The certification must be signed and submitted by a duly authorized representative for the bidder.

☐ **EXHIBIT A-2 – BIDDER'S PROFILE AND REFERENCES**

This document is required bidder information for the WSIB contract administration purposes. Complete as instructed and submit with the bid to the WSIB.

☐ **EXHIBIT B – QUESTIONNAIRE**

Bidder will need to provide responses to the questions in Exhibit B – Questionnaire**.**

☐ **EXHIBIT C – FEE SCHEDULE**

Bidder will need to complete the price worksheet templates as instructed in ***Exhibit C – Fee Schedule***.

☐ **EXHIBIT D – WORK ORDER #24-01 [PROPOSED CHANGES IF APPLICABLE]**

WSIB reserves the right to modify the terms and conditions to ensure compliance with state law or policy. If the bidder has business concerns or other issues with the terms and conditions in Exhibit D - Work Order #24-01 the bidder must provide proposed changes within the form in MS Word format. If no changes are submitted the bidder therefore agrees to the contract as drafted. The WSIB will not thereafter consider substantive changes to Exhibit D.

4.4. **BID FORMAT**. Bids must be complete and must follow all instructions stated in the ITPS Work Request (including the exhibits). Unless otherwise specified in writing by the WSIB, documents included with an electronic bid must be prepared in MS Word, MS Excel, or Adobe PDF. Where required to do so, bidders may sign using either a physical or electronic signature.

4.5. **SUBMITTING BIDS**. Your electronic bid must be emailed to Contracts@sib.wa.gov. Email boxes can only accept emails that are less than 30MB in size. Bidders are cautioned to keep email sizes to less than 25MB to ease delivery. Zipped files will not be accepted.

SECTION 5 – COMPLAINT, DEBRIEF, & PROTEST REQUIREMENTS

This section details the applicable requirements for complaints, debriefs, and protests.

5.1. **COMPLAINTS**. This Solicitation offers a complaint period for bidders wishing to voice objections to this solicitation. The complaint period ends five (5) business days before the bid due date. The complaint period is an opportunity to voice objections, raise concerns, or suggest changes that were not addressed during the Question & Answer Period or, if applicable, at the Pre-Bid Conference. Failure by the bidder to raise a complaint at this stage may waive its right for later consideration. The WSIB will consider all complaints but is not required to modify or cancel the ITPS Work Request. If bidder complaints result in changes written amendment(s) will be issued and posted on WEBS.

a. **CRITERIA FOR COMPLAINT**. A formal complaint may be based only on one or more of the following grounds: (a) The solicitation unnecessarily restricts competition; (b) The solicitation evaluation or scoring process is unfair or flawed; or (c) The solicitation requirements are inadequate or insufficient to prepare a response.

b. **INITIATING A COMPLAINT**. A complaint must: (a) Be submitted to and received by the Procurement Coordinator no less than five (5) business days prior to the deadline for bid submittal; and (b) Be in writing (see Form and Substance, and Other below). A complaint should clearly articulate the basis of the complaint and include a proposed remedy.

c. **RESPONSE**. When a complaint is received, the Procurement Coordinator (or designee) will consider all the facts available and respond in writing prior to the deadline for bid submittals, unless more time is needed. The WSIB is required to promptly post the response to a complaint on WEBS.

d. **RESPONSE IS FINAL**. The Procurement Coordinator's response to the complaint is final and not subject to administrative appeal. Issues raised in a complaint may not be raised again during the protest period. Furthermore, any issue, exception, addition, or omission not brought to the attention of the Procurement Coordinator prior to bid submittal may be deemed waived for protest purposes.

5.2. **DEBRIEF CONFERENCES**. A Debrief Conference is an opportunity for a bidder and the WSIB through its Procurement Coordinator, to meet and discuss the bidder's bid (and, as further explained below, is a necessary prerequisite to filing a protest). Following the evaluation of the bids, the WSIB will issue an announcement of the ASB. That announcement may be made by any means, but the WSIB likely will use email to the bidder's

email address provided in the Bidder's Profile. Bidders will have three (3) business days to request a Debrief Conference. Once a Debrief Conference is requested, the WSIB will offer the requesting bidder one meeting opportunity and notify the bidder of the Debrief Conference place, date, and time. Please note, because the debrief process must occur before making an award, the WSIB likely will schedule the Debrief Conference shortly after the announcement of the ASB and the bidder's request for a Debrief Conference. The WSIB will not allow the debrief process to delay the award. Therefore, bidders should plan for contingencies and alternate representatives. **Bidders who wish to protest must first participate in a debrief conference. Bidders who are unwilling or unable to attend the Debrief Conference will lose the opportunity to protest. A debrief is a required prerequisite for a bidder wishing to file a protest**.

a. **TIMING**. A Debrief Conference may be requested by a bidder following announcement of the Apparent Successful Bidder (ASB).

b. **PURPOSE OF DEBRIEF CONFERENCE**. Any bidder who has submitted a timely bid response may request a Debrief Conference (see Form and Substance, and Other below). A Debrief Conference provides an opportunity for the bidder to meet with the WSIB to discuss bidder's bid and evaluation. It does not provide an opportunity to discuss other bids and evaluations.

c. **REQUESTING A DEBRIEF CONFERENCE**. The request for a Debrief Conference must be made in writing via email to the Procurement Coordinator and received within three (3) business days after the announcement of the Apparent Successful Bidder. Debrief conferences will be conducted virtually (e.g., by telephone or web-based virtual meeting such as Zoom, Skype, MS Teams), as determined by the WSIB, and may be limited by the WSIB to a specified period of time. The failure of a bidder to request a debrief within the specified time and attend a debrief conference constitutes a waiver of the right to submit a protest. Any issue, exception, addition, or omission not brought to the attention of the procurement coordinator before or during the debrief conference may be deemed waived for protest purposes.

5.3. **PROTESTS**. Following a Debrief Conference, a bidder may protest the award of a Contract.

a. **CRITERIA FOR A PROTEST**. A protest may be based only on one or more of the following: (a) Bias, discrimination, or conflict of interest on the part of an evaluator; (b) Error in computing evaluation scores; or (c) Non-compliance with any procedures described in the Competitive Solicitation.

b. **INITIATING A PROTEST**. Any bidder may protest an award to the ASB. A protest must: (a) Be submitted to and received by the Procurement Coordinator within five (5) business days after the protesting bidder's Debriefing Conference (see Form and Substance, and Other below); (b) Be in writing; (c) Include a specific and complete statement of facts forming the basis of the protest; and (d) Include a description of the relief or corrective action requested.

c. **PROTEST RESPONSE**. After reviewing the protest and available facts the WSIB will issue a written response within ten (10) business days from receipt of the protest, unless additional time is needed.

d. **DECISION IS FINAL**. The protest decision is final and not subject to administrative appeal. If the protesting bidder does not accept the protest response, the bidder may seek relief in Thurston County Superior Court.

5.4. **COMMUNICATION DURING COMPLAINTS, DEBRIEFS, AND PROTESTS**. All communications about this ITPS Work Order, including complaints, debriefs, and protests, must be addressed to the Procurement Coordinator unless otherwise directed.

a. **FORM, SUBSTANCE, & OTHER**. All complaints, requests for debrief, and protests must:

i. Be in writing.

ii. Be signed by the complaining or protesting bidder or an authorized agent, unless sent by email.

iii. Be delivered within the time frame(s) outlined herein.

iv. Identify the Solicitation number.

v. Conspicuously state "Complaint," "Debrief," or "Protest" in any subject line of any correspondence or email.

vi. Be sent to the address identified below.

b. **COMPLAINTS & PROTESTS**. All complaints and protests must (a) State all facts and arguments on which the complaining or protesting bidder is relying as the basis for its action; and (b) Include any relevant documentation or other supporting evidence.

5.5. **HOW TO CONTACT THE WSIB**.

a. **TO SUBMIT A COMPLAINT**. Send an email message to the Procurement Coordinator at the following email address: Contracts@sib.wa.gov. The email message must include "Complaint" in the subject line of the email message.

b. **TO REQUEST A DEBRIEF CONFERENCE**. Send an email message to the Procurement Coordinator at the following email address: Contracts@sib.wa.gov. The email message must include "Debrief" in the subject line of the email message.

c. **TO SUBMIT A PROTEST**. Send an email message to Procurement Coordinator at the following email address: Contracts@sib.wa.gov . The email message must include "Protest" in the subject line of the email message. Alternatively, mail the protest at the following address:

SECTION 6 – DOING BUSINESS WITH THE STATE OF WASHINGTON

This section provides additional information regarding Washington's Public Records Act and doing business with the State of Washington, including the WSIB's efforts to enable Washington's small, diverse, and veteran-owned businesses to compete for and participate in state procurements for services.

6.1. **WASHINGTON'S PUBLIC RECORDS ACT – PUBLIC RECORDS DISCLOSURE REQUESTS**.

- All documents (written and electronic) submitted as part of this procurement are public records. Unless statutorily exempt from disclosure, such records are subject to disclosure ***if*** requested. *See* RCW 42.56, Public Records Act. The WSIB strongly discourages bidders from unnecessarily submitting sensitive information (e.g., information that bidder might categorize as 'confidential,' 'proprietary,' 'sensitive,' 'trade secret,' etc.).
  - If, in bidder's judgment, Washington's Public Records Act provides an applicable statutory exemption from disclosure for certain portions of bidder's bid, please mark the precise portion(s) of the relevant page(s) of the bid that bidder believes are statutorily exempt from disclosure and identify the precise statutory basis for exemption from disclosure.
  - In addition, if, in bidder's judgment, certain portions of bidder's bid are not statutorily exempt from disclosure but are sensitive because these particular portions of bidder's bid (NOT including pricing) include highly confidential, proprietary, or trade secret information (or the equivalent) that bidder protects through the regular use of confidentiality or similar agreements and routine enforcements through court enforcement actions, please mark the precise portion(s) of the relevant page(s) of bidder's bid that include such sensitive information.
- In the event that the WSIB receives a public records disclosure request pertaining to information that bidder has submitted and marked either as (a) statutorily exempt from disclosure; or (b) sensitive, prior to disclosure, will do the following:
  - The WSIB's Public Records Officer will review any records marked by bidder as statutorily exempt from disclosure. In those situations, where the WSIB concludes the designation comports with the stated statutory exemption from disclosure, the WSIB will redact or withhold the document(s) as appropriate.
  - For documents marked 'sensitive' or for documents where the WSIB either determines that no statutory exemption to disclosure applies or is unable to determine whether the stated statutory exemption to disclosure properly applies, the WSIB will notify bidder, at the email address provided in

the bid submittal, of the public records disclosure request and identify the date that the WSIB intends to release the document(s) (including documents marked 'sensitive' or exempt from disclosure) to the requester unless the bidder, at bidder's sole expense, timely obtains a court order enjoining the WSIB from such disclosure. In the event bidder fails to timely file a motion for a court order enjoining such disclosure, the WSIB will release the requested document(s) on the date specified. Bidder's failure properly to identify exempted or sensitive information and timely respond after notice of request for public disclosure has been given shall be deemed a waiver by bidder of any claim that such materials are exempt or protected from disclosure.

6.2. **SMALL & DIVERSE BUSINESSES**. The WSIB, in accordance with Washington law, encourages small and diverse businesses to compete for and participate in state procurements as contractors and as subcontractors to awarded bidders. *See, e.g.*, RCW 39.19 (OMWBE certified businesses); RCW 43.60A.200 (WDVA certified veteran-owned businesses); and RCW 39.26.005 (Washington small businesses).

- OMWBE CERTIFICATION. Bidders may contact the Washington State Office of Minority and Women's Business Enterprises (OMWBE) regarding information on Minority-Owned and Women-Owned certified firms, state and federal certification programs, or to become certified. OMWBE can be reached by telephone, 866-208-1064, or through their website at OMWBE. OMWBE-Certified firms may provide their certification information on ***Exhibit A-2 – Bidder's Profile and References***.
- WDVA CERTIFICATION. Bidders may contact the Washington State Department of Veterans' Affairs (WDVA) for information regarding Certified Veteran-Owned businesses or to become a Certified Veteran-Owned Business. The WDVA can be reached by telephone, (360) 725-2169, or through their website at WDVA. WDVA Certified firms may provide their certification information in ***Exhibit A-2 – Bidder's Profile and References***.
- WASHINGTON SMALL BUSINESSES. Bidders may contact the WSIB about small and diverse business inclusion and qualification as a Washington Small Business. If you qualify as a Washington Small Business, identify yourself as such in WEBS. Call WEBS Customer Service at 360-902-7400. The qualification requirements to self-certify as a Washington Small Business are set forth in ***Exhibit A-1 – Bidder's Certification***.

6.3. **WEBS REGISTRATION**. Individuals and firms interested in state contracting opportunities with any state agency should register for Solicitation notices at the Washington Electronic Business Solution (WEBS) WEBS Registration. *Note*: There is no cost to register on WEBS.

ITPS WORK REQUEST #24-01

ATTACHMENT A

WASHINGTON STATE INVESTMENT BOARD

RECOMMENDED REAL ESTATE INTERMEDIARY

CONTROL GUIDELINES

SEPTEMBER 2021

CONTROL GUIDELINES OVERVIEW

This document provides a framework for the design and implementation, or assessment and enhancement, of risk management and internal control processes. These guidelines are applicable for the Washington State Investment Board (WSIB) Real Estate Investment Intermediary Managers (the "Intermediary"), relating to how they manage the "Company" or "Companies", and the investments i.e., the Real Estate Operating Companies (the "REOCs").

The "Control Self-Assessment" section of this document captures risk management and internal control "best practices". It is intended as a tool to assist each Intermediary with maintaining strong controls and risk management practices. The Control Self-Assessment is incorporated into each Company's Annual Plan, which is a statement confirming completion of a control self-assessment by the Intermediary.

RISK MANAGEMENT AND INTERNAL CONTROL FRAMEWORKS

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations, established in the United States, dedicated to providing thought leadership to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. COSO has established a common internal control model against which companies and organizations may assess their control systems. The WSIB believes COSO provides good guidance for the Intermediaries to use when managing a Company or REOC.

FRAMEWORK COMPONENTS AND PRINCIPLES

The COSO internal control framework consists of five interrelated components derived from the way management runs an organization. According to COSO, these components provide an effective framework for describing and analyzing internal control systems. COSO has also defined best practice principles in organizations for effective enterprise risk management. The internal control and risk management components and principles described by COSO are summarized below.

CONTROL ENVIRONMENT:

- The organization demonstrates a commitment to integrity and ethical values.
- The board of directors demonstrates independence from management, carries out risk governance responsibilities to support management achieving strategy and business objectives and exercises oversight of the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of strategy and business objectives.
- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with strategy and business objectives.
- The organization defines the desired behaviors that characterize the entity's core values and attitudes toward risk.
- The organization holds individuals at all levels accountable for their risk management and internal control responsibilities and holds itself accountable for providing standards and guidance.

RISK ASSESSMENT:

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to the business objectives at various levels that align with and support strategy.
- The organization defines risk appetite in the context of creating, preserving, and realizing value.

- The organization identifies risks in execution that impact the achievement of business objectives across the entity, analyzes severity, and prioritizes risks as a basis for determining how the risks should be managed.
- The organization identifies and selects risk responses.
- The organization considers the potential for fraud in assessing risks to the achievement of objectives.
- The organization identifies and assesses changes that could impact the system of internal control or the risk profile.

CONTROL ACTIVITIES:

- The organization selects and develops control activities that mitigate risks to acceptable levels.
- The organization selects and develops general control activities over technology to support the achievement of objectives.
- The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

INFORMATION AND COMMUNICATION:

- The organization uses relevant, quality information to support the functioning of other components of risk management and internal control.
- The organization internally communicates information, including objectives and responsibilities for risk management and internal control, necessary to support the functioning of risk management and internal control.
- The organization reports on risk, culture, and performance at multiple levels and across the entity.
- The organization communicates with external parties regarding matters affecting the functioning of other components of risk management and internal control.

MONITORING:

- The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of risk management and internal control are present and functioning.
- The organization assesses operating performance results and considers risk.
- The organization evaluates and communicates risk management and internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board, as appropriate.

For more information on COSO, please see the following website: COSO.org.

CONTROL SELF-ASSESSMENT

The following sections outline the framework Intermediaries can use to manage and operate the Companies, and assess current controls, identify gaps, and consider action plans to address.

I. INSURANCE

Intermediary insurance coverage is reviewed annually for adequacy, and includes … cybersecurity … coverage.

II. CONFIDENTIAL INFORMATION

A. Adequate procedures are in place to safeguard private information.

The Intermediary should undertake reasonable measures to protect the confidentiality and security of information.

B. Media communications policies exist for Intermediary employees, which include guidelines for … social media use.

Identification of the types of information that can and cannot be disclosed on Company social media accounts (if applicable), as well as employees' personal social media profiles helps to minimize security risk and protect the business from legal issues. Potential disciplinary actions if social media posts affect the organization's image are also included in policy.

III. INFORMATION SYSTEMS

A. The Intermediary is using best-in-class technology and applications, commensurate with the maturity of the Company and its underlying investments.

B. Security Controls: The Intermediary has adopted an IT security policy, defined data classification scheme, change management process, and security controls relating to the following are in place.

1. Logical controls. The Intermediary has established logical access controls which focus on data, systems, file organizations, etc.

    a. Access to computers, servers, and systems that contain confidential and/or critical data are restricted using unique user identification, passwords, and firewalls.

Measures to ensure strong/secure passwords include:

- First-time passwords set to a unique value per user that must be changed immediately after first use.
- A minimum password length of 10 characters, with at least three of the following character classes included: uppercase letters, lowercase letters, numerals, and special characters.
- Individuals are prohibited from submitting a new password that is the same as any of the previous four passwords used by the individual.
- A maximum of five incorrect login attempts are allowed, before the account is locked for a minimum of 15 minutes or until reset by an administrator.
- Pass codes used to secure mobile devices

- Are a minimum of six:
  - Alpha numeric characters (highly recommended), containing at least three unique character classes; **OR**
  - Digits with mandatory use of biometric authentication for all users.
- Do not contain more than a three consecutive character run. Pass codes consisting of 123467, 1234!a, or abcd1! are not acceptable.
- Render the device unusable after 10 failed login attempts.

b. Multi-factor authentication is enabled whenever available for logging into programs/ systems used by the Company.

c. Systems provide the ability to:

- Authenticate users.
- Audit access and changes to data.
- Restrict or grant users' privileges in accessing and changing data based on their roles.

d. Access to systems is based on the principle of least privilege where users are granted the minimum level of access needed to perform required tasks.

e. System-generated access security reports are monitored and reviewed at least annually to ensure the access levels/rights of all users are appropriate given their respective job duties. Reviews are also conducted when staff leave the organization and/or job duties change. These reviews are documented and include, at a minimum, the accounting and online banking systems.

2. Physical controls. The Intermediary has controls over physical information system resources which take into consideration how secure these resources are against physical dangers such as theft, based upon a vulnerability and risk assessment.

Physical access to data centers and computer systems (including laptops and mobile devices) that contain confidential and critical data should be safeguarded to protect against theft. Employees are required to report a lost or missing mobile device to the IT department immediately.

3. Cybersecurity. The Intermediary has named a cybersecurity lead. Training of Intermediary employees regarding relevant cybersecurity risks to the Company achieving its objectives, and their role in reducing these risks, is conducted annually and participation documented.

a. A process and corresponding set of controls designed to ensure all software within Company control is kept up to date is in place. This includes a patching cycle/policy for all Company devices, including servers, computers, and mobile devices that ensures timely, regular updates.

b. End users should not have administrative rights to endpoint devices.

c. Users that have a need for administrative access rights have a *separate* administrative account.

Administrator account credentials are separate from standard user credentials; and administrator accounts are not used for non-administrative purposes.

d. Tools are in place to assist with monitoring for breach activity.

Independent vulnerability assessments, or more robust continuous monitoring tools to gather data focused on identification of anomalies may be warranted.

e. A formal incident response policy and plan are in place to provide guidance in the event of a cybersecurity (or other suspected fraud) incident. Periodic tests of the incident response plan and procedures ensure the plan is kept current.

In the event of a cybersecurity incident, the Intermediary will follow-up to identify attackers, and/or gaps in the control structure that need to be resolved to avoid recurrence. All cybersecurity incidents are reported to the respective federal Internet Crime Compliance Center as soon as possible to assist with recovery of funds.

C. Backup and Recovery: Steps are taken by the Intermediary to ensure proper and timely recovery of its information systems.

This includes safeguarding records against potential loss or destruction by fire, theft, vandalism, storm, earthquake, terrorism, tsunami, or any other hazard. Backup and recovery procedures are established. There is a plan for business continuation in emergency situations, and periodic tests of the plan and procedures ensure the plan is kept current.

IV. ONGOING REOC MONITORING

The Intermediary ensures adequate risk management and internal control processes applicable to the underlying REOC businesses are in place and operating effectively. Guidance provided to the REOCs incorporates the controls and risk management practices included in this document, as well as industry best practices related to areas of operations that are unique to REOC businesses (e.g., accounts receivable).