

Request For Proposal

Solicitation number: DOR-WR K2104

Fraud Analyst – Ron Sampson

for

Washington State Department of Revenue (DOR)

Table of Contents

No. 1 -Signed Executive Summary – Section II, subsection 11. A.3
 Guidacent ThreatRecon Cybersecurity Practice4
 Guidacent Cybersecurity Consulting Pedigree4
No. 2 - Bidder References – Section II, subsection 11. B.6
No. 3 - Cost – Section II, subsection 11. C.7
No. 4 - Proposed Staff Qualifications – Section II, subsection 11. D.8
 Guidacent Resume – Ronald Sampson10
No. 5 - Proposed Staff References – Section II, subsection 11. E.12
No. 6 -Signed Certifications and Assurances Form – Section II, subsection 11. F.13
No. 7 - Bidder /certification form Executive Order 18-03 Workers’ Rights – Section II, subsection 11. G. 14
No. 8 - Bidder Certification form Wage Theft Prevention – Section II, subsection 11. H.....15
No. 9 - Covid 19 Vaccination Requirement – Section II, subsection 11. I.....16

EXECUTIVE SUMMARY which includes the following information stated in a concise manner and formatted to facilitate review of the material.

Question	Guidacent Response
Bidder Name, FEIN, UBI, address, phone, and representative’s name and contact information.	Guidacent, Inc. FEIN: 45-3720106 UBI: 603 154 118 10900 Northeast 4th Street Suite 2300 Bellevue, WA 98004 425-655-2992 Representative: Bob Morgan Managing Partner bob.morgan@guidacent.com 206-931-8788 (M)
Date Bidder is available to start work, if selected	December 1, 2022
Brief description of the company	<p>Guidacent is a Washington State-based business and technology professional consulting and advisory services firm that specializes in implementing solutions with seasoned leaders to solve business challenges. Guidacent’s primary mission is to improve client success through trusted, scalable, measurable, and timely services, which focus on blended solutions that impact three key areas: Project Management, Data Integrity, and Cybersecurity. For more than a decade, Guidacent’s pool of veteran consultants help clients from multiple industries deliver mission-critical solutions to achieve their organizational goals. The following image illustrates some of our key service-line offerings.</p> <p>Guidacent is currently working with WSDOT and have received positive feedback related to the work we are engaged in the upgrading of their financial management software.</p> <div data-bbox="867 1402 1284 1864" data-label="Diagram"> <p>The diagram consists of a central dark blue hexagon with the text 'Consulting Services' and a mountain logo. It is surrounded by six light blue hexagons, each containing a service name: 'Project Rescue' (top), 'Cybersecurity Risk Management' (top-right), 'Supply Chain Efficiency' (bottom-right), 'Cloud Transformation Services' (bottom), 'Business Intelligence & Analytics' (bottom-left), and 'Framework Architecture' (top-left). The 'Cybersecurity Risk Management' hexagon is outlined in red.</p> </div>

Question	Guidacent Response
<p>Description of Bidder’s experience and history providing Fraud Analyst services for large complex information technology projects.</p>	<p>Guidacent ThreatRecon™ Cybersecurity Practice</p> <p>Our ThreatRecon™ Cybersecurity Practice offers a highly focused portfolio of risk advisory and threat mitigation services that impacts customer defenses from the first day.</p> <p>These services assist Guidacent clients in their efforts to reduce the risk of a compromise associated with fraud and continue advancing their business operations. Evaluating and improving existing security governance — with focus on Fraud Prevention, Data Privacy, and regulatory compliance — are core tenets of the ThreatRecon™ portfolio.</p> <p>Guidacent Cybersecurity Consulting Pedigree</p> <p>Electronic fraud affects a wide span of business operations across all sectors—especially financial and insurance-centric organizations. Guidacent’s ThreatRecon cybersecurity division considers the issue of “online fraud” as one of the key areas of concern that continues to escalate as a primary target point within business operations. Our approach to addressing this rapidly growing problem is based on ITIL, NIST and ISO guidelines for electronic fraud and aligned topics, Specific to the Healthcare Sector, ThreatRecon Fraud Analysts incorporate HIPAA and HIRUST guidelines and best practices. Guidacent’s team of ThreatRecon Fraud Analysts include:</p> <ul style="list-style-type: none"> • Contributing to establishing the CVE standard for evaluating all cybersecurity attacks and vulnerabilities. • Authors of the Health Information Portability and Accountability Act (HIPAA). • Member organizers of the Department of Homeland Security. • Founding the industry’s first hacker research team and event (DefCon / Black Hat Briefings). • Founding members of the RSA Conference (more than 40,000 attendees annually). • Establishing post-graduate degree programs at universities in the U.S. and Asia. • Planning & developing the structure for establishing a multi-site “follow-the-sun” Secure Operations Center for one of the world’s leading auto manufacturers. • Former application CISOs for the world’s largest franchise. • Deputy CISOs for global retail, “big box” and cruise lines. • Architects of cybersecurity “Zero Trust” Architectures for large health care organizations. • Former U.S. Department of Defense Information Warfare Specialists. • Contributing editors to the CISSP, CEH and Purdue CERIAs programs.

Question	Guidacent Response
Name, title, and signature of person with authority to enter into a Contract on behalf of the Bidder.	Robert Vandersluis Director Robert.Vandersluis@guidacent.com 206-498-9116 (M) Signature:  Robert Vandersluis

Bidder References, DOR requires the Bidder to provide three (3) references from clients who engaged Bidder specific to Fraud Analyst services and/or similar work. References must include the following, in order listed:

Question	Guidacent Response
Reference 1	
Organization Name	Glance Networks
Organization Website Address	https://ww2.glance.net
Contact Name and Title	Byron K. Thomas, Solutions Architect, ISMS Manager
Contact Phone Number	(617) 852-1329
Contact Email Address	bthomas@glance.net
Name and Brief Description of the Project(s)	Fraud/Cybersecurity workshop We sought Guidacent's Cybersecurity expertise by contracting Guidacent to do a 3- day Fraud/Cybersecurity workshop that included a tabletop ransomware attack exercise
Reference 2	
Organization Name	Nutanix - Enterprise Cloud - Run Any Application at Any Scale
Organization Website Address	https://www.nutanix.com
Contact Name and Title	Alexandra Adams
Contact Phone Number	425-449-6867
Contact Email Address	Alexandra.huft@nutanix.com
Name and Brief Description of the Project(s)	Security Projects and Tools Implementation Management of several detailed security projects as well as implementation of supporting tools.
Reference 3	
Organization Name	Nutanix - Enterprise Cloud - Run Any Application at Any Scale
Organization Website Address	https://www.nutanix.com
Contact Name and Title	Adam McDaid, Manager, Technical Programs
Contact Phone Number	202-813-5545
Contact Email Address	Adam.mcdaid@nutanix.com
Name and Brief Description of the Project(s)	Compliance Projects Compliance and development of automated cloud asset tracking mechanism

COST. Fixed Hourly rate for each proposed Bidder(s). Indicate if Bidder is proposing a team or offering multiple staff for evaluation.

Guidacent is presenting the below Fraud Analyst to work with the DOR

Guidacent, Inc - Cost -

Resource Name	Title/Role	Hourly Rate
Ronald Sampson	Fraud Analyst	\$160

PROPOSED CONSULTANT QUALIFICATIONS, which includes the following information stated in a concise manner and formatted to facilitate review of the material:

Question	Guidacent Response
Consultant Name	Ron Sampson
Number of years' experience providing Professional Expert Level Fraud Analyst services for a high dollar, multi-year system implementation projects, noting the number of those years were for government projects	15 years' working extensively with major organizations in the finance industry to manage structure, design implement processes, conduct compliance audits, and evaluations.
Education	Rutgers - New Brunswick, NJ Bachelor of Arts in Communications
Certifications, including year received	<ul style="list-style-type: none"> • Certified Data Privacy Solutions Engineer (CDPSE) – 1/28/2018 • Certified Information Systems Manager (CISM) -4/9/2020 • Certified Information Systems Auditor (CISA) – 9/17/2020 • Certified Identity and Access Manager (CIAM) – 9/17/202

List three (3) projects proposed staff provided Professional Expert Level Fraud Analyst services for, including the following information:	
Project #1 – Name:	IT Process and Controls
Project Objective	Performed IT/Data access risk assessments using corporate methodology to identify, document and communicate control deficiencies in processes and technology systems.
Project Start and End Dates	2012 - 2017
Describe proposed staff role and responsibilities on each project, the length of the engagement, and if the proposed staff completed the engagement	<ul style="list-style-type: none"> • Managed a team of 5 external consultants through the full audit cycle. • Identified and tested key controls, processes, and key risk indicators. • Identified customer transaction patterns indicative of suspicious activity and investigated inappropriate and/or fraudulent activity. • Created charts and reports to present to Sr. Management • Verified and tested adherence to Technology Risk governance • This was a five (5)-year project and completed by the staff.
Project Budget	Budget covered project start and end dates
Summary of qualifications, to include knowledge of Fraud Analyst services, management, and supervisory responsibilities	<ul style="list-style-type: none"> • Preparation of detailed investigation reports • Provided services around process and controls matrix, controls testing and the review and challenge of First Line testing methodology and results. • Collaborated with stakeholders to analyze investigations results, identifying trends and define typologies within the bank's footprint that could harbor money laundering or terrorist financing activity

Project #2 – Name:	Global IT Security
Project Objective	Provide controls, policy, and procedure testing, monitoring and enterprise risk management
Project Start and End Dates	2017 - 2020
Describe proposed staff role and responsibilities on each project, the length of the engagement, and if the proposed staff completed the engagement	<ul style="list-style-type: none"> • Developed and updated DRP and BCP policies and procedures to ensure compliance with new regulations to close regulator audit findings report. • Worked with business teams to identify, document and provide governance of information risk models across the enterprise. • Provided QA and validation of enterprise information risk score changes to detect trends and annual refresh of the GISR score. • This engagement was completed.
Project Budget	Budget covered project start and end dates
Summary of qualifications, to include knowledge of Fraud Analyst services, management, and supervisory responsibilities	<ul style="list-style-type: none"> • Project resulted in increased use of the application risk score across the enterprise to assess and mitigate risk across 11 business units.

Project #3 - Name	SLOD (Second Line of Defense) Challenge and Oversight
Project Objective	Provide management and oversight of enterprise application information security risk assessments.
Project Start and End Dates	2020 -
Describe proposed staff role and responsibilities on each project, the length of the engagement, and if the proposed staff completed the engagement	<ul style="list-style-type: none"> • Support ongoing strategic planning for IT Risk Management programs, policies, and procedure to ensure alignment with regulatory requirements. • Ongoing evaluation of IT and security controls • Project is ongoing
Project Budget	Project budgeted through duration of time
Summary of qualifications, to include knowledge of Fraud Analyst services, management, and supervisory responsibilities	<ul style="list-style-type: none"> • Document and provide governance of information risk models. • Work with stakeholders to remediate gaps and implement improvements in control design, process, and performance. • Compliance Risk Manager Responsibilities

Note: The Bidder must provide DOR with resumes for the proposed resources. The resumes must outline how they meet or exceed the minimum requirements specified in this Work Request.

Ronald Sampson

SUMMARY

Experienced Information Security Controls Officer with more than 15 years of experience helping clients implement the tools and governance necessary particularly in the finance industry. Strong skills in the management and oversight of enterprise application information security risk assessments, vendor assessments, compliance audits and evaluations in accordance with applicable IT process/risk/control frameworks (NIST, COBIT, ITIL, COSO).

- Risk Assessment and Management
- Identity and Access Management
- Compliance Management
- Information Security
- Security Analysis
- Internal Audits

PROFESSIONAL EXPERIENCE

USAA, ITCSC Compliance Risk Manager Lead 2020- Present

Project: Responsible for Enterprise IT Compliance conducting Second Line of Defense (SLOD) challenge and oversight.

- SLOD management and oversight of enterprise application information security risk assessments, vendor assessments, compliance audits and evaluations in accordance with applicable IT process/risk/control frameworks (NIST, COBIT, ITIL, COSO).
- Provided design and implementation of QA/QC processes through ongoing SLOD monitoring and testing of Information Security and Identity & Access Management (IAM) controls.
- Conducted controls test planning and execution of controls testing in accordance with the banks established processes and procedures.
- Support ongoing strategic planning for IT Risk Management programs, policies, and procedures to ensure alignment with regulatory requirements and risk reduction best practices.
- Implemented strong project execution which resulted in an increase in completed risk assessments and build out of the Asset Management and Configuration Management Risk and Controls matrices. Additional results in an increased compliance with FFIEC and NYDFS regulations.

Bank of America, Information Security Controls Officer 2017 – 2020

Project: Design and implementation of QA/QC processes through ongoing SLOD monitoring and testing of Information Security and Identity & Access Management (IAM) controls.

- Managed a team of five (5) tasked with providing effective SLOD governance, monitoring and testing and communication across the organization.
- Managed Global IT Security providing controls, policy and procedure testing, monitoring and enterprise risk management.
- Developed updated Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) policies and procedures to ensure compliance with new regulations and best practices.
- Results increased alignment and compliance with FFIEC and bank Disaster Recovery and Business Continuity rules and regulations which were used to satisfy and close regulator audit findings report.
- Provided QA and validation of enterprise information risk score changes, quarterly analysis of changes to detect trends and annual refresh of the GISR score inputs/calculations to ensure the score is measuring risk of current threat environment.

-
- Worked with Business Controls Management & Readiness team to identify, document and provide governance of information risk models across the enterprise.
 - Project resulted in increased use of the application risk score across the enterprise to assess and mitigate risk across 11 business units.
 - Designed test plans/scripts and identified appropriate testing population and scope.
 - Identified gaps and implemented control improvements for operational excellence initiatives across the enterprise.

Gallop Solutions, Information Security Consultant 2012-2017

Project: Provided IT Consulting for several major banking clients (Bank of America, Chase, Citi & NationStar) to help implement process and controls matrix builds, controls testing and review and challenge of First Line testing methodology and results.

- Performed IT/Data access risk assessments using corporate methodology to identify, document and communicate control deficiencies in processes and technology systems.
- The results helped increase data security and lower data incidents based on adding additional controls and increasing oversight of enterprise systems and data.
- Managed a team of 5 external consultants through the full audit cycle including identifying and testing key controls, processes, and key risk indicators in accordance with GTO Policy and Standards and/or ITIL framework and ISACA Control Objectives for Information and Related Technologies (COBIT).
- These results provided a significant reduction of regulator audits in direct response to the design and effectiveness of controls testing program established by the team.

EDUCATION & CERTIFICATIONS**Rutgers University**

Bachelor of Arts, Communications

- CDPSE - Certified Data Privacy Solutions Engineer since 1/28/2018
- CISM (Certified Information Systems Manager) since 4/9/2020
- CISA (Certified Information Systems Auditor), CIAM (Certified Identity and Access Manager) since 9/17/2020

PROPOSED STAFF REFERENCES: THREE (3) REFERENCES, FOR EACH PROPOSED STAFF. Please include the following in the order listed:

Proposed Staff Name: Ron Sampson

Question	Guidacent Response
Organization Name	Bank of America
Organization Website Address	https://www.bankofamerica.com/
Contact Name and Title	Carnis Jefferson, Audit Manager
Contract Phone Number	704-458-5314
Contact Email Address	carnis.jefferson@gmail.com
Name and Brief Description of the Project(s)	IT Audit
Bidder must also included signed Certifications and Assurances form Attachment B.	Please see signed Certifications and Assurances form Attachment B

Question	Guidacent Response
Organization Name	Bank of America
Organization Website Address	https://www.bankofamerica.com/
Contact Name and Title	Ayo Daniels, IT Controls Manager
Contract Phone Number	614-596-6995
Contact Email Address	danofx1@yahoo.com
Name and Brief Description of the Project(s)	Cyber security and controls
Bidder must also included signed Certifications and Assurances form Attachment B.	Please see signed Certifications and Assurances form Attachment B

Question	Guidacent Response
Organization Name	Mondov Group
Organization Website Address	
Contact Name and Title	David Cox
Contract Phone Number	862-201-9340
Contact Email Address	turnipseed30@yahoo.com
Name and Brief Description of the Project(s)	Compliance Consulting
Bidder must also include signed Certifications and Assurances form Attachment B.	Please see signed Certifications and Assurances form Attachment B

ATTACHMENT B: CERTIFICATIONS AND ASSURANCES

I/we make the following certifications and assurances as a required element of the proposal to which it is attached, understanding that the truthfulness of the facts affirmed here and the continuing compliance with these requirements are conditions precedent to the award or continuation of the related contract:

I/we declare that all answers and statements made in the proposal are true and correct.

1. The prices and cost data have been determined independently, without consultation, communication, or agreement with others for the purpose of restricting competition. However, I/we may freely join with other persons or organizations for the purpose of presenting a single proposal.
2. The attached proposal is a firm offer for a period of ninety (90) days following receipt, and it may be accepted by the Washington State Department of Revenue (DOR) without further negotiation (except where obviously required by lack of certainty in key terms) at any time within the ninety (90)-day period.
3. In preparing this proposal, I/we have not been assisted by any current or former employee of the state of Washington whose duties relate (or did relate) to this proposal or prospective contract, and who was assisting in other than his or her official, public capacity. If there are exceptions to these assurances, I/we have described them in full detail on a separate page attached to this document.
4. I/we understand that DOR will not reimburse me/us for any costs incurred in the preparation of this proposal. All proposals become the property of DOR, and I/we claim no proprietary right to the ideas, writings, items, or samples, unless so stated in this proposal.
5. Unless otherwise required by law, the prices and cost data which have been submitted have not been knowingly disclosed by the Proposer and will not knowingly be disclosed by him/her prior to opening, directly or indirectly, to any other Proposer or to any competitor.
6. I/we agree that submission of the attached proposal constitutes acceptance of the solicitation contents and the attached sample contract and general terms and conditions. If there are any exceptions to these terms, I/we have described those exceptions in detail on a page attached to this document.
7. No attempt has been made or will be made by the Proposer to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.
8. I/we grant DOR the right to contact references and others, who may have pertinent information regarding our ability to perform the services requested in this Work Request (WR).

We (circle one) **are / are not** submitting proposed Contract exceptions. If Contract exceptions are being submitted, I/we have attached them to this form.

On behalf of the Bidder submitting this proposal, my name below attests to the accuracy of the above statement. We are submitting a scanned signature of this form with our proposal.



Signature of Bidder

November 3, 2022

Date

Director

Title

ATTACHMENT D

WORKERS' RIGHTS CERTIFICATION

I hereby certify, on behalf of the firm identified below, as follows (check one):

NO MANDATORY INDIVIDUAL ARBITRATION CLAUSES AND CLASS OR COLLECTIVE ACTION WAIVERS FOR EMPLOYEES. This firm does NOT require its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waivers.

OR

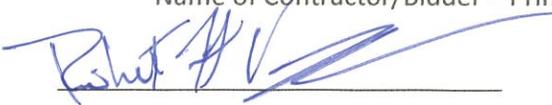
MANDATORY INDIVIDUAL ARBITRATION CLAUSES AND CLASS OR COLLECTIVE ACTION WAIVERS FOR EMPLOYEES. This firm requires its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waivers.

I hereby certify, under penalty of perjury under the laws of the State of Washington, that the certifications herein are true and correct and that I am authorized to make these certifications on behalf of the firm listed herein.

Solicitation No.: DOR-WR-K2104

FIRM NAME: Guidacent, Inc

Name of Contractor/Bidder – Print full legal entity name of firm

By: 
Signature of authorized person

Robert Vandersluis
Print Name of person making certifications for firm

Title: Director
Title of person signing certificate

Place: Bellevue, WA
Print city and state where signed

Date: November 3, 2022

ATTACHMENT C - CONTRACTOR CERTIFICATION

WAGE THEFT PREVENTION – RESPONSIBLE BIDDER CRITERIA

WASHINGTON STATE GOODS & SERVICES CONTRACTS

Prior to awarding a contract, agencies are required to determine that a bidder is a ‘responsible bidder.’ See RCW 39.26.160(2) & (4). Pursuant to legislative enactment in 2017, the responsible bidder criteria include a contractor certification that the contractor has not willfully violated Washington’s wage laws. See Chap. 258, 2017 Laws (enacting SSB 5301).

Solicitation No.: **Work Request DOR-WR-K104 for Fraud Analyst**

Solicitation Date: **October 14, 2022**

I/we hereby certify, on behalf of the firm identified below, as follows (check one):

NO WAGE VIOLATIONS. This firm has NOT been determined by a final and binding citation and notice of assessment issued by the Washington Department of Labor and Industries (LNI) or through a civil judgment entered by a court of limited or general jurisdiction to have willfully violated, as defined in RCW 49.48.082, any provision of RCW chapters 49.46, 49.48, or 49.52 within three (3) years prior to the date of the above-referenced procurement solicitation date.

OR

VIOLATIONS OF WAGE LAWS. This firm has been determined by a final and binding citation, and notice of assessment issued by the Washington Department of Labor and Industries (LNI) or through a civil judgment entered by a court of limited or general jurisdiction to have willfully violated, as defined in RCW 49.48.082, a provision of RCW chapters 49.46, 49.48, or 49.52 within three (3) years prior to the date of the above-referenced procurement solicitation date.

I hereby certify, under penalty of perjury under the laws of the State of Washington, that the certifications herein are true and correct and that I am authorized to make these certifications on behalf of the firm listed herein.

FIRM NAME: GUIDACENT, INC _____
Name of Contractor/Bidder – Print full legal entity name of firm

By:  _____
Signature of authorized person

Robert Vandersluis _____
Print Name of person making certifications for firm

Title: Director _____
Title of person signing certificate

Place: Bellevue, WA _____
Print city and state where signed

Date: November 3, 2022

Attachment F

Contractor Certification

Proclamation 21-14 - COVID-19 Vaccination Certification

To reduce the spread of COVID-19, Washington state Governor Jay Inslee, pursuant to emergency powers authorized in RCW 43.06.220, issued Proclamation 21-14 – COVID-19 Vaccination Requirement (dated August 9, 2021), as amended by Proclamation 21-14.1 – COVID-19 Vaccination Requirement (dated August 20, 2021) and as may be amended thereafter. The Proclamation requires contractors who have goods, services, or public works contracts with a Washington state agency to ensure that their personnel (including subcontractors) who perform contract activities on-site comply with the COVID-19 vaccination requirements, unless exempted as prescribed by the Proclamation.

Department of Revenue (“DOR”) Contract Number: K2104

I hereby certify, on behalf of the firm identified below, as follows (check one):

CONTRACTOR HAS A COVID-19 CONTRACTOR VACCINATION VERIFICATION PLAN THAT COMPLIES WITH THE VACCINATION PROCLAMATION. Contractor:

- *Has reviewed and understands Contractor’s obligations as set forth in Proclamation 21-14 – COVID-19 Vaccination Requirement (dated August 9, 2021), as amended by Proclamation 21-14.1 – COVID-19 Vaccination Requirement (dated August 20, 2021);*
- *Has developed a COVID-19 Vaccination Verification Plan for Contractor’s personnel (including subcontractors) that complies with the above-referenced Proclamation;*
- *Has obtained a copy or visually observed proof of full vaccination against COVID-19 for Contractor personnel (including subcontractors) who are subject to the vaccination requirement in the above-referenced Proclamation;*
- *Complies with the requirements for granting disability and religious accommodations for Contractor personnel (including subcontractors) who are subject to the vaccination requirement in the above-referenced Proclamation;*
- *Has operational procedures in place to ensure that any contract activities that occur in person and on-site at DOR premises (other than only for a short period of time during a given day and where any moments of close proximity to others on-site will be fleeting – e.g., a few minutes for deliveries) that are performed by Contractor personnel (including subcontractors) will be performed by personnel who are fully vaccinated or properly exempted as required by the above-referenced Proclamation;*
- *Has operational procedures in place to enable Contractor personnel (including subcontractors) who perform contract activities on-site and at DOR premises to provide compliance documentation that such personnel are in compliance with the above-referenced Proclamation;*

Attachment F

Contractor Certification

Proclamation 21-14 - COVID-19 Vaccination Certification

Page 2

- Will provide to DOR, upon request, Contractor’s COVID-19 Vaccination Verification Plan and related records, except as prohibited by law, and will cooperate with any investigation or inquiry pertaining to the same.

OR

- CONTRACTOR DOES NOT HAVE A COVID-19 CONTRACTOR VACCINATION VERIFICATION PLAN.* Contractor does not have a current COVID-19 Contractor Vaccination Verification Plan and is not able to develop and provide a COVID-19 Contractor Vaccination Verification Plan to ensure that Contractor’s personnel (including subcontractors) meet the COVID-19 vaccination requirements as set forth in the above-referenced Proclamation and provide the same to DOR within twenty-four (24) hours of such designation. [Note: Compliance with the Proclamation is mandatory.]

I hereby certify, under penalty of perjury under the laws of the State of Washington, that the certifications herein are true and correct and that I am authorized to make these certifications on behalf of the firm listed herein.

Solicitation No.: DOR-WR-K2104

Solicitation Date: October 14, 2022

Firm Name: Guidacent, Inc. _____
Name of Contractor – Print full legal entity name of firm

By: 
Signature of authorized person

Robert Vandersluis
Print Name of person making certifications for firm

Title: Director
Title of person signing certificate

Place: Bellevue, WA
Print city and state where signed

Date: November 3, 2022

Return to Procurement & Contracts Manager
Department of Revenue
LoriG@dor.wa.gov
Post Office Box 47462
Olympia, WA 98504

Failure to submit may result in contract termination.