



Commonwealth of Kentucky

MASTER AGREEMENT

CONTRACT INFORMATION

MASTER AGREEMENT NUMBER: MA 758 2300000427

Effective Date: 10/01/2022

Record Date: 09/21/2022

Expiration Date: 04/04/2027

Procurement Folder: 965205

Document Description: NASPO ValuePoint Software Value Added
Reseller-All State MA

Procurement Type: Special Authority Goods & Svcs

Cited Authority: Intergovernmental Purchases

Version Number: 1

CONTACT INFORMATION

ISSUER:

Susan Noland
502-564-5951
Susan.Noland@ky.gov

VENDOR INFORMATION

Name /Address:

KY0028837: Insight Public Sector Inc
6820 S. Harl Ave.
Tempe AZ 85283

Contact:

Accounts Receivable
1-800-INSIGHT
teamhazzard@insight.com

COMMODITY / SERVICE INFORMATION

Line	Quantity	UOM	Unit Price	Service Amount	Service From	Service To	Line Total
1	0.00000		\$0.000000	\$0.00			\$0.00

Software Value Added Reseller-All State Agency

Extended Description:

Software Value Added Reseller
See header for executed Participating Addendum.
All State Agency

	Document Description	Page 2
2300000427	NASPO ValuePoint Software Value Added Reseller-All State MA	

NASPO ValuePoint COOPERATIVE PURCHASING PROGRAM
Software Value Added Reseller (SVAR)
Lead State (Arizona)
NASPO Master Agreement: CTR060025
Kentucky Master Agreement: MA 758 2300000427

Terms and Conditions

Please click the link below for additional NASPO ValuePoint contractual information and terms and conditions related to the procurement and award of the contracts.

<https://www.naspovaluepoint.org/portfolio/software-var/insight/>

Software Value Added Reseller (SVAR)

The expiration date of this contract is April 4, 2027. There are two (2) optional 1-year extensions.

See Header of the MA for executed Participating Addendum

All documentation is on file in OPS.

**PARTICIPATING ADDENDUM
NASPO VALUEPOINT**

Software Value Added Reseller (SVAR)

Administered by the State of Arizona (hereinafter “Lead State”)

MASTER AGREEMENT

Insight Public Sector, Inc.

Master Agreement No: CTR060025

(hereinafter “Contractor”)

And

Commonwealth of Kentucky

(hereinafter “Participating State”)

Commonwealth Master Agreement No: MA 758 2300000427

This Participating Addendum is entered into by Contractor and Participating Entity (collectively, the “Parties”).

Scope and Participation:

1. Scope: This addendum covers the Software Value Added Reseller contract led by the State of Arizona for use by state agencies and other entities located in the Participating State authorized by that state’s statutes to utilize State contracts with the prior approval of the state’s chief procurement official.

Category I – General Software (Maximum Markup per Attachment B)

Category II – Microsoft-Software (Maximum Markup per Attachment B)

Maximum Markup is the Maximum Markup on Reseller’s Invoiced Cost

☐ This Participating Addendum includes the entire scope of the products and services available through the Master Agreement referenced above.

☒ This Participating Addendum includes the entire scope of the products and services available through the Master Agreement referenced above, except the following:

- *Leasing Option (Section 2.2.2.9)*
- *The Commonwealth reserves the right to add Category III – Oracle Products and Services at a later date, if it is in the best interest of the Commonwealth.*

Any scope exclusions specified herein apply only to this Participating Addendum and shall not amend or affect other participating addendums or the Master Agreement itself.

2. Participation: Use of specific NASPO ValuePoint cooperative contracts by agencies, political subdivisions and other entities (including cooperatives) authorized by an individual state’s statutes to use State contracts are subject to the prior approval of the respective State Chief

Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

3. Term:

☒ The term of this Participating Addendum shall begin on October 1, 2022, through April 24, 2027. The term shall continue for a period ending on the Termination Date of the Master Agreement or when this Participating Addendum is terminated in accordance with the Master Agreement, whichever shall occur first.

4. Primary Contacts: The following (or their named successors) are the primary contact individuals for this Participating Addendum:

CONTRACTOR:

Name:	Brittany Dunaway
Address:	2701 E. Insight Way, Chandler, AZ 85286
Telephone:	480.366.7029
Fax:	480.760.9957
Email:	SLEDcontracts@insight.com

PARTICIPATING ENTITY:

Name:	Susan S. Noland
Address:	200 Mero Street, 5 th Floor, Frankfort, KY 40622
Telephone:	(502) 564-5951
Fax:	N/A
Email:	Susan.Noland@ky.gov

Participating Entity Modifications and Additions to the Master Agreement

☐ This Participating Addendum incorporates all terms and conditions of the Master Agreement as applied to the Participating Entity and Contractor.

☒ This Participating Addendum incorporates all terms and conditions of the Master Agreement as applied to the Participating Entity and Contractor, **subject to the following limitations, modifications, and additions:**

The following changes are modifying or supplementing the Master Agreement terms and conditions

- a. Section 2.5.2.1 & Section 2.5.1 General Requirements – All Categories
 - The website shall provide contract and quote information only. No online ordering is permitted. Commonwealth agencies must use the Commonwealth's

eprocurement system for all ordering. The using agency will create a Delivery Order in the eprocurement system and send to the reseller to initiate the order. The reseller shall not process any orders without a Delivery Order.

- b. Section 2.5.2.1 - Online Product Quotes
 - Commonwealth agencies are permitted to obtain online quotes however no online ordering is permitted. Commonwealth agencies must use the Commonwealth's eprocurement system for all ordering. The using agency will create a Delivery Order in the eprocurement system and send to the reseller to initiate the order. The reseller shall not process any orders without a Delivery Order.
- c. Section 2.5.2.4 - Guaranteed 60 Day Quote
 - The reseller shall honor all quotes for sixty (60) calendar days.
- d. Section 2.5.6.1 – Dedicated Representation and Timely Response
 - The reseller must commit to returning phone calls or responding to emails within one (1) business day.
- e. The Commonwealth's Master Agreement number (MA 758 2300000427) must be referenced on all quotes and invoices.
- f. Any End User License Agreement (EULA) should be submitted with the quote and reference the Commonwealth's Master Agreement number (MA 758 2300000427). All EULAs shall be governed by the laws of the Commonwealth of Kentucky. Any action brought against the Commonwealth regarding the agreement, including but not limited to actions either for breach of agreement or for enforcement of the agreement, shall be brought in Franklin Circuit Court, Franklin County, Kentucky in accordance with KRS 45A.245.
- g. The reseller shall send the Commonwealth Office of Technology (COT) invoices to: COT.Invoices@ky.gov. Other Commonwealth using agencies' invoices shall be sent to the email addresses/addresses located on the using agencies' Delivery Order.
- h. The reseller shall send all order confirmations and license keys to the requesting agency along with including COTAsset.Software@ky.gov
- i. The Commonwealth shall only make payment to the reseller and not the software publishers/vendors. All payments shall be net thirty (30) days.
- j. The reseller shall comply with the Commonwealth Office of Technology (COT) policies and standards when applicable (see Attachment A of this document).
- k. The reseller shall accept purchasing credit cards as a form of payment without charging any fees for the purchase.
- l. The reseller agrees to provide a quarterly administrative fee to the Participating State as part of the reseller's unit prices and is not to be charged directly to Participating Entities in the form of a separate line item. The administrative fee shall be paid in the form of a check payable to the Office of Procurement Services for an amount equal to one percent (1%) of the net sales (less any returns, credits or adjustments) under this Participating Addendum for the period. Fees shall be paid 45 days after the close of the quarter. Check to be mailed to the Office of Procurement Services, 200 Mero Street, 5th Floor, Frankfort, KY 40622 to the attention of Susan S. Noland. Quarterly sales reports shall be emailed to Susan.Noland@ky.gov.
- m. The participating state is agreeing to the terms of the NASPO Master Agreement only to the extent the terms are not in conflict with state and federal law, inclusive of any Commonwealth of Kentucky procurement statutes and regulations.
- n. Governing Law. This Participating Addendum shall be governed and construed in

accordance with the laws of the Commonwealth of Kentucky per KRS 45A. Parties agree that this Addendum is subject to Kentucky State law and any provision of the Addendum that is in direct conflict with any applicable Kentucky State law shall be deemed unenforceable.

Any limitations, modifications, or additions specified herein apply only to the agreement and relationship between Participating Entity and Contractor and shall not amend or affect other participating addendums or the Master Agreement itself.

5. Lease Agreements: Lease Agreements are not permitted under this PA.
6. Subcontractors: All contactors, dealers, and resellers authorized in the Commonwealth of Kentucky, as shown on the dedicated Insight Public Sector (cooperative contract) website, are approved to provide sales and service support for participants in the NASPO ValuePoint Master Agreement. The Insight Public Sector dealer's participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement.
7. Orders: Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.

Attachment A

Commonwealth Office of Technology (COT) Policies and Standards

1. Commonwealth Information Technology Policies and Standards

- A. The vendor and any subcontractors shall be required to adhere to applicable Commonwealth policies and standards.
- B. The Commonwealth posts changes to COT Standards and Policies on its [Commonwealth Office of Technology - Home - Commonwealth Office of Technology \(Kentucky\)](#) website. Vendors and subcontractors shall ensure their solution(s) shall work in concert with all posted changes. Vendors or subcontractors that cannot comply with changes must, within thirty (30) days of the posted change, request written relief with the justification for such relief. The Commonwealth may 1) deny the request, 2) approve an exception to the policy / standard, or 3) consider scope changes to the contract to accommodate required changes. Vendors or subcontractors that do not provide the response within the thirty (30) day period shall be required to comply within ninety (90) days of the change.

2. Compliance with Kentucky Information Technology Standards (KITS)

- A. The Kentucky Information Technology Standards (KITS) reflect a set of principles for information, technology, applications, and organization. These standards provide guidelines, policies, directional statements and sets of standards for information technology. It defines, for the Commonwealth, functional and information needs so that technology choices can be made based on business objectives and service delivery. The vendor shall stay knowledgeable and shall provide a solution that works in concert with these standards for all related work.
<https://technology.ky.gov/about-the-agency/Pages/kits.aspx>
- B. The vendor and any subcontractors may be required to submit a technology roadmap for any offered solution. Additional roadmaps will be submitted upon request of the Commonwealth. The Roadmap shall include, but is not limited to, planned, scheduled and projected product lifecycle dates and historical release/patch or maintenance dates for the technology. In addition, any guidance on projected release/revision/patch/maintenance schedules would be preferred.

3. Compliance with Commonwealth Security Standards

The software deployment and all vendor services shall abide by privacy and security standards as outlined in the Commonwealth's Enterprise Information Technology Policies.

Enterprise Security Policies

<https://technology.ky.gov/OCISO/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx>

Enterprise IT Policies

<https://technology.ky.gov/policies-and-procedures/Pages/policies.aspx>

4. Compliance with Industry Accepted Reporting Standards Based on Trust Service Principles and Criteria

The vendor must employ comprehensive risk and threat management controls based on defined industry standards for service organizations such as ISO AICPA TSP section 100, Trust Services Principles and Criteria. The vendor must annually assert compliance and engage a third party certification registrar to examine such assertions and controls to provide a Report, such as ISO 9000, ISO 14001, AT101 SOC 2 type 2, on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy, which contains an opinion on whether the operating controls effectively support the assertions. All such reports, including publicly available reports (i.e. AT 101 SOC 3) shall be made available to the Commonwealth for review.

5. System Vulnerability and Security Assessments

The Commonwealth reserves the right to conduct, in collaboration with the vendor, non-invasive vulnerability and security assessments of the software and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of these assessments, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls that will reduce risk to an acceptable and agreed upon level. An accredited third party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

6. Privacy Assessments

The Commonwealth reserves the right to conduct Privacy assessments of the collection, use, maintenance and sharing of Commonwealth data by any vendor services, software, and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of this assessment, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls or privacy practices that will reduce risk to an acceptable and agreed upon level. An accredited third party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

7. Privacy, Confidentiality and Ownership of Information

The Commonwealth is the designated owner of all Commonwealth data and shall approve all access to that data. The vendor shall not have ownership of

Commonwealth data at any time. The vendor shall not profit from or share Commonwealth data. The vendor shall be in compliance with privacy policies established by governmental agencies or by state or federal law. Privacy notice statements may be developed and amended from time to time by the Commonwealth and will be appropriately displayed on the Commonwealth portal (Ky.gov). The vendor should provide sufficient security to protect the Commonwealth and COT data in network transit, storage, and cache. **All Commonwealth data, including backups and archives, must be maintained at all times within the contiguous United States. All Commonwealth data, classified as sensitive or higher, as defined in Enterprise Standards, must be encrypted in-transit from Contractor's network and at rest while stored on Contractor's laptops or other portable media devices.**

8. **EU GDPR Compliance, if applicable**

The Commonwealth of Kentucky requires all vendor contracts to comply with the European Union's General Data Privacy Regulation [Regulation (EU) 2016/679] (the "GDPR") when the Commonwealth is a "controller" or "processor" of "personal data" from an individual "data subject" located in the European Union, as those terms are defined in the GDPR. The Contractor acknowledges and agrees that it is acting as a "processor" of "personal data" for the Commonwealth under this Agreement and that all applicable requirements of the GDPR are incorporated by reference as material terms of this Agreement. The Contractor represents and warrants that (1) it is aware of and understands its compliance obligations as a "processor" under GDPR; (2) it has adopted a GDPR compliance policy/program, a copy of which has been provided to the Commonwealth; (3) it will process "personal data" only in accordance with the Commonwealth's instructions; and (4) with regard to its obligations under this Agreement, it shall comply with all applicable requirements of the GDPR to the same extent as adopted by the Commonwealth. Additionally, the Contractor shall indemnify and hold harmless the Commonwealth, and its employees from and against any claims, demands, suits, damages, penalties, fines, or costs arising from any violation of GDPR by the Contractor.

9. **Data Quality**

The vendor shall provide proposed levels of data quality per the following dimensions.

Data Quality is the degree to which data is valid, accurate, complete, unique, timely, consistent with all requirements and business rules, and relevant for a given use. The vendor shall provide data quality definitions and metrics for any data elements. Data has to be of the appropriate quality to address the needs of the Commonwealth of Kentucky. The following dimensions can be used to assess data quality:

- Validity – The data values are in an acceptable format.
- Accuracy – The data attribute is accurate.
- Completeness – There are no null values in a data field.
- Uniqueness – There are no duplicate values in a data field.
- Timeliness – The data attribute represents information that is not out-of-date.

- Consistency – The data attribute is consistent with a business rule that may be based on that attribute itself, or on multiple attributes.
- Adherence to business rules – The data attribute or a combination of data attributes adheres to specified business rules.

10. Metadata Requirement

The vendor shall provide a glossary for all business terms used in this solution.

11. Software Development

Source code for software developed or modified by the vendor specifically for the Commonwealth shall become property of the Commonwealth. This is not meant to include minor modifications to the vendor software to configure the software for Commonwealth use. This is meant to include software written to add functionality to the vendor product specifically to meet the requirements of the Commonwealth where the Commonwealth bears the entire cost of creating that functionality.

12. License Agreements

Software provided by the vendor to the Commonwealth should contain a provision for perpetual licensing with all upgrade options. License agreements should also contain a provision for the Commonwealth to maintain a version of the software in escrow in the event the vendor is unable to continue business for financial or other business reasons.

Any escrow agreement shall be negotiated by all parties.

Any third party software licenses and cloud resources necessary for the proposed solution may be procured via the Commonwealth's existing contracts.

13. Software Version Requirements

All commercially supported and Commonwealth approved software components such as Operating system (OS), Database software, Application software, Web Server software, Middle Tier software, and other ancillary software must be kept current. In the event that a patch interferes with the solution, the vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution in to compliance to allow this patch to be applied in the shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

The Vendors shall keep software in compliance with industry standards to support third party products such as Java, Internet Explorer, Mozilla Firefox, etc. at latest supported version, release, and patch levels, when such dependencies exist. In the event that a third party dependency interferes with the solution, the vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution into compliance to allow this third party dependency to be

updated in the shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

14. No Surreptitious Code Warranty

The contractor represents and warrants that no copy of licensed Software provided to the Commonwealth contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this contract as the "No Surreptitious Code Warranty".

As used in this contract, "Self-Help Code" means any back door, time bomb, drop-dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access) for purposes of maintenance or technical support.

As used in this contract, "Unauthorized Code" means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code.

In addition, contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the Commonwealth.

The vendor shall defend the Commonwealth against any claim, and indemnify the Commonwealth against any loss or expense arising out of any breach of the No Surreptitious Code Warranty.

15. OS Requirements

a. Non-On Prem Solutions

1. No Commonwealth data shall be co-mingled with another entity, without the prior approval of the Commonwealth.
2. Vendor shall provide a solution to move data to the Commonwealth, if required by the Commonwealth.
 - a. At the end of the contract, the vendor shall provide all agency data in a useable standard data format (such as ascii, csv, etc.) that can be converted to a subsequent system. The vendor shall cooperate to this end with the Agency and/or a vendor of the agency's choice, in a timely and efficient manner.
 - b. Vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The vendor shall cooperate to this end with the vendor of the agency's choice, in a timely and efficient manner.
 - c. Vendor shall provide address the destruction of Commonwealth data as defined in CIO-092 and provide a certification of the complete and permanent deletion the Commonwealth data.

B. Infrastructure As A Service

1. Vendor shall work with the Agency and COT to establish all administrative personnel engagements.
2. All virtual environments must run on VMC (VMWare Cloud) with OS version compliant with KITS, unless explicitly approved by COT.
3. VMC shall provide an enterprise class malicious code protective solution that is currently supported by the vendor and up to date
4. Vendor shall meet certification requirements for classification of data being stored.
5. Vendor shall, at COT's request, provide appropriate access to enable the Commonwealth to perform additional security measures in compliance with Commonwealth Enterprise Policies, Standards, and/or any Federal or State requirements.
6. Vendor shall provide an Exit Strategy, to move all data to the Commonwealth Data Center, if required by the Commonwealth.
 - a. At the end of the contract, the vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The vendor shall cooperate to this end with the Vendor of the agency's choice, in a timely and efficient manner.
 - b. Vendor shall provide certification of the complete and permanent deletion of Commonwealth data and backups from all vendor storage.

16. Project Governance

Vendor shall work with the Agency and appropriate COT offices, when needed, in the cases of data governance, security aspects, hosting, integration, etc., provided that such work does not expand the scope of the services absent a corresponding change order agreed to by the parties reflecting such expansion.

17. Project Management Requirements

The COT Division of Governance and Strategy (COT-DGS) is responsible for overseeing large and complex technology projects throughout the Commonwealth. The vendor shall adhere to Project Management standards and reporting requirements established by COT-DGS, which are posted at <https://technology.ky.gov/services-and-support/Pages/About-the-Project-Management-Branch.aspx>. These include, but are not limited to, having a documented project schedule, risk management, issue management and reporting project status to the CIO monthly in the format defined by COT-DGS. In addition to the project management standards required by COT-DGS, agency specific requirements may be defined.

18. Applicable Security Control Framework Compliance

The vendor must have an awareness and understanding of the NIST Special Publication 800-53 Security Control Framework and employ safeguards that meet or exceed the moderate level controls as defined within the standard. The respondent must provide sufficient safeguards to provide reasonable protections around the Commonwealth's data to ensure that the confidentiality, integrity, and availability is maintained at an appropriate level. These include but are not limited to:

- *Access Control*
The vendor must employ policy and process that provide for stringent control to limit physical and logical access to systems that house Commonwealth data, on a need to know basis, provide clear separation of duties, and adheres to least privilege principles.
- *Awareness and Training*
The vendor must provide the appropriate role specific training for staff to ensure that there is awareness and understanding of roles and responsibilities as they relate to the protections around the Commonwealth's data.
- *Audit and Accountability*
There must be sufficient auditing capability to ensure that actions are tracked and there is individual accountability for all actions taken by vendor staff.
- *Configuration Management*
The vendor must work within established baselines that provide minimal functionality needed to ensure service delivery without exposing unnecessary risk. The vendor must also employ structured change control processes that provide a level of coordination with the client agreed upon in a Service Level Agreement (SLA).
- *Contingency Planning*
The vendor must employ contingent planning policy and procedures that ensure service delivery based on agreed SLA levels while maintaining all Commonwealth data within the continental United States.
- *Identification and Authorization*
The vendor must employ appropriate identity and access management policies and procedures to ensure that access is appropriately authorized and managed at a level to ensure that access is provisioned and de-provisioned in a timely and efficient manner.
- *Incident Response*
The vendor must employ policy and procedures to ensure that an appropriate response to all identified security incidents are addressed in a timely manner and are reported to the appropriate parties in an agreed upon SLA timeframe. The vendor must also ensure that all staff are sufficiently trained to ensure that they can identify situations that are classified as security incidents.
- *Maintenance*
The vendor must employ policy and procedures that ensure that all maintenance activities are conducted only by authorized maintenance staff leveraging only authorized maintenance tools.
- *Media Protection*
The vendor must employ policy and procedure to ensure that sufficient protections exist to protect Commonwealth data on all storage media throughout the media lifecycle and maintain documentation from media creation through destruction.
- *Physical and Environmental Controls*
The vendor must employ physical and environmental policies and procedures that ensure that the service and delivery infrastructure are located in a physically secure and environmentally protected environment to ensure the confidentiality, integrity, and availability of Commonwealth data.

- *Personnel Security*
The vendor must employ policies and procedures to ensure that all staff that have access to systems that house, transmit, or process Commonwealth data have been appropriately vetted and have been through a background check at the time of hire and periodically thereafter.
- *System and Communications Protections*
The vendor must employ physical and logical protection that protect system communications and communication media from unauthorized access and to ensure adequate physical protections from damage.

Attachment B – Pricing Sheet

INSIGHT PUBLIC SECTOR NASPO VALUEPOINT SOFTWARE VALUE-ADDED RESELLER (SVAR) STATE OF KENTUCKY CONTRACT # MA 758 2300000427 ALL PUBLISHERS <u>EXCEPT</u> MICROSOFT AND ORACLE	
PUBLISHERS	MAXIMUM MARKUP ON RESELLER'S INVOICED COST
Tier I Publishers (Key Itemized Publishers)	
ADOBE	2.00%
CA TECHNOLOGIES (acquired by Broadcom)	2.00%
CISCO	1.95%
COMMVAULT	1.95%
IBM	2.00%
RED HAT	1.95%
SPLUNK	2.00%
TABLEAU	2.00%
VEEAM	1.95%
VMWARE	1.95%
Tier II Publishers (Other Itemized Publishers)	
AUTODESK	2.50%
BARRACUDA NETWORKS	2.50%
BMC SOFTWARE	2.25%
CHECK POINT SOFTWARE	2.50%
CHERWELL	2.25%
CITRIX	2.25%
CHATSWORTH PRODUCTS (CPI)	2.25%
CROWDSTRIKE	2.25%
DELL	2.25%
DELPHIX	2.25%
DOCUSIGN	2.50%
DYNATRACE	2.50%
FORCEPOINT	2.50%
FORTINET	2.25%
GOOGLE	2.25%
INFORMATICA	2.50%
IVANTI	2.50%
KNOWBE4	2.50%
MCAFEE	2.25%
MICRO FOCUS	2.50%
MULESOFT	2.25%
NETMOTION	2.50%
OKTA	2.25%
OPENTEXT	2.50%
PROGRESS SOFTWARE	2.50%
PROOFPOINT	2.25%
QUEST SOFTWARE	2.50%
RAPID7	2.50%
RSA SECURITY	2.50%
SALESFORCE	2.50%
SAP	2.50%
SOLARWINDS	2.50%
SOPHOS	2.50%

SPILLMAN (acquired by Motorola Solutions)	2.25%
SYMANTEC (acquired by Broadcom)	2.50%
TENABLE	2.50%
TREND MICRO	2.50%
VARONIS	2.50%
VERITAS	2.25%
ZOHO	2.50%
Non-itemized Publishers	
All other publishers	4.75%

INSIGHT PUBLIC SECTOR NASPO VALUEPOINT SOFTWARE VALUE-ADDED RESELLER (SVAR) STATE OF KENTUCKY CONTRACT # MA 758 2300000427 ALL PUBLISHERS <u>EXCEPT</u> MICROSOFT AND ORACLE	
RESELLER SERVICES	HOURLY RATE
Asset management	\$200.00
Solutions architect	\$209.00
Senior solutions architect	\$265.00
Program engagement manager	\$232.00
Project leader	\$127.00
Project manager	\$209.00
Senior project manager	\$220.00
All other in-scope reseller services (Connected Workforce / Cloud + Data Center Transformation)	\$284.00
OPTIONAL SERVICES	HOURLY RATE
Digital Innovation: UX/Visual/Product	
Creative Director	\$325.00
Principal Designer	\$300.00
Associate Creative Director	\$300.00
Design Manager	\$275.00
Product Manager	\$275.00
Senior Designer	\$250.00
Senior Business Analyst	\$250.00
Designer	\$225.00
Business Analyst	\$225.00
Associate Designer	\$190.00
Associate Business Analyst	\$190.00
Digital Innovation: PM	
Services Manager	\$325.00
Program Manager	\$250.00
Project Manager	\$225.00
Project Coordinator	\$190.00
Digital Innovation: Technology	
Principal/Chief Architect	\$325.00
Senior Architect	\$300.00
Managing Architect	\$300.00
Architect	\$275.00
Senior Software Engineer	\$250.00
Software Engineer	\$225.00
Associate Software Engineer	\$190.00

INSIGHT PUBLIC SECTOR NASPO VALUEPOINT SOFTWARE VALUE-ADDED RESELLER (SVAR) STATE OF KENTUCKY CONTRACT # MA 758 2300000427 MICROSOFT	
SUBCATEGORY	MAXIMUM MARKUP ON RESELLER'S INVOICED COST
Itemized Microsoft Offerings	
EMS E5, G1, G2, G3, G5, Govt E4, Advanced Threat Protection, Power BI, Exchange Online, Kiosk F3 Now, Dynamics, PowerApps, Project Online, Azure	1.65%
All Other Microsoft Offerings	
SaaS	1.65%
On-Premise	1.65%
Resold In-scope Professional Services	
Ongoing maintenance & support services not included in software license agreement	1.65%
Deployment services	1.65%
Architectural design services	1.65%
Training deployment services	1.65%
All other resold in-scope professional services	1.65%
IN-SCOPE RESELLER SERVICES	HOURLY RATE
Asset management	\$200.00
Solutions architect	\$209.00
Senior solutions architect	\$265.00
Program engagement manager	\$232.00
Project leader	\$127.00
Project manager	\$209.00
Senior project manager	\$220.00
All other in-scope reseller services (Connected Workforce / Cloud + Data Center Transformation)	\$284.00
OPTIONAL SERVICES	MAXIMUM MARKUP ON
Cloud Solution Provider (CSP) Program (SaaS only)	15.00%
OPTIONAL SERVICES	HOURLY RATE
Digital Innovation: UX/Visual/Product	
Creative Director	\$325.00
Principal Designer	\$300.00
Associate Creative Director	\$300.00
Design Manager	\$275.00
Product Manager	\$275.00
Senior Designer	\$250.00
Senior Business Analyst	\$250.00
Designer	\$225.00
Business Analyst	\$225.00
Associate Designer	\$190.00
Associate Business Analyst	\$190.00
Digital Innovation: PM	
Services Manager	\$325.00
Program Manager	\$250.00
Project Manager	\$225.00
Project Coordinator	\$190.00
Digital Innovation: Technology	
Principal/Chief Architect	\$325.00
Senior Architect	\$300.00
Managing Architect	\$300.00
Architect	\$275.00

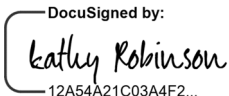
Senior Software Engineer	\$250.00
Software Engineer	\$225.00
Associate Software Engineer	\$190.00

IN WITNESS WHEREOF, the Parties have executed this Participating Addendum.

PARTICIPATING ENTITY

CONTRACTOR

Signature: 	Signature: 
Name: Jim Barnhart	Name: Lianne Steinheiser
Title: Deputy CIO	Title: Global Compliance Officer
Date: 9-21-22	Date: 9/20/2022

Participating State: Commonwealth of Kentucky Office of Procurement Services (OPS)
BY:  12A54A21C03A4F2...
Name: Kathy Robinson
Title: Executive Director
Date: 9/21/2022

For questions regarding NASPO ValuePoint Participating Addendums, please contact the Cooperative Contract Coordinator team at info@naspovaluepoint.org.

Fully executed NASPO ValuePoint Participating Addendums must be submitted via email in PDF format to pa@naspovaluepoint.org.