



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 5

List View

General Information

Contact

Default Values

Discount

Document Information

Procurement Folder: 619426

SO Doc Code: CRFQ

Procurement Type: Central Master Agreement

SO Dept: 0210

Vendor ID: VS0000020805

SO Doc ID: ISC2000000011

Legal Name: CASEPOINT LLC

Published Date: 1/23/20

Alias/DBA:

Close Date: 1/30/20

Total Bid: \$4,800.00

Close Time: 13:30

Response Date: 01/23/2020

Status: Closed

Response Time: 14:54

Solicitation Description: Addendum 4-e-Discovery
Softw are as a Service (OT19141)

Total of Header Attachments: 5

Total of All Attachments: 5



Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 619426

Solicitation Description : Addendum 4-e-Discovery Software as a Service (OT19141)

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-01-30 13:30:00	SR 0210 ESR01232000000004307	1

VENDOR

VS0000020805
CASEPOINT LLC

Solicitation Number: CRFQ 0210 ISC2000000011

Total Bid : \$4,800.00 Response Date: 2020-01-23 Response Time: 14:54:08

Comments:

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Signature on File

FEIN #

DATE

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Contract Services: e-Discovery System	100.00000	EA	\$12.000000	\$1,200.00

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :	Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in
-------------------------------	---

Comments: Unit price listed is per gb per month.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Opt Renewal Y2: Contract Services: e-Discovery System	100.00000	EA	\$12.000000	\$1,200.00

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :	Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in
-------------------------------	---

Comments: Unit price listed is per gb per month.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Opt Renewal Y3: Contract Services: e-Discovery System	100.00000	EA	\$12.000000	\$1,200.00

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :	Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in
-------------------------------	---

Comments: Unit price listed is per gb per month.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Opt Renewal Y4: Contract Services: e-Discovery System	100.00000	EA	\$12.000000	\$1,200.00

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :	<p>Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line</p> <p>The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in</p>
------------------------	--

Comments: Unit price listed is per gb per month.



West Virginia Office of Technology Request for Quotation (RFQ)

For an eDiscovery Software as a Service

January 16, 2020



Company Name: Casepoint, LLC

Company Address: 7900 Tysons One Place, Suite 680
Tysons, VA 22120

Company Website: <http://www.casepoint.com>

Authorized Representative: Amy Hilbert
Vice President, Public Sector
Mobile: 443-506-8219
Office: 703-738-4220
Email: ahilbert@casepoint.com

01/16/2020

Jessica Chambers
Jessica.S.Chambers@wv.gov
2019 Washington Street, East
Charleston, WV 25305

Re: CRFQ ISC2000000011–eDiscovery Software Solution for the West Virginia Office of Technology

Dear Ms. Chambers,

Casepoint, LLC ("Casepoint") is pleased to present our solution to implement our eDiscovery Tool to support the West Virginia Office of Technology with an eDiscovery Software as a Service. Attached with our response, please find:

- A copy of Casepoint's Terms and Conditions that the State of West Virginia or Agency will have to agree to as part of this solicitation (PDF)
- Bid Documents with completed information and required signatures (PDF)
- Addenda Acknowledgement
- W-9 Form

As the company point of contact, I have provided my contact information below if you have any questions.

Sincerely,



Amy Hilbert
Vice President, Public Sector
Casepoint, LLC
7900 Tysons One Pl Suite 680
Tysons, VA 22102
Phone: 703-738-4408
Fax: 844-882-0022
Email: ahilbert@casepoint.com

Table of Contents

1	Executive Summary.....	1
1.1	About Casepoint.....	3
2	Qualifications & Requirements.....	4
3	Casepoint eDiscovery	6
3.1.1	Data Ingestion and Processing.....	7
3.1.2	Document Review.....	8
3.1.3	Analytics and Artificial Intelligence	10
3.1.4	Productions	15
3.1.5	User Access and Security	16
4	Previous Casepoint Implementations	16

1 Executive Summary

The West Virginia Office of Technology (WVOT) is seeking an eDiscovery software as a service to use for the varying needs and challenges related to discovery in legal proceedings. Because the WVOT needs to balance increasing eDiscovery needs within fixed and sometimes shrinking budget constraints, the WVOT needs a robust, scalable, and cost-effective eDiscovery platform with a depth of functionalities and features including, self-service data ingestion and processing, advanced analytics, full-strength document review and production powerful analytics.

Why Casepoint is the best eDiscovery Solution for the West Virginia Office of Technology







Casepoint is a unified eDiscovery platform that can be shared across parties to efficiently review millions of electronically stored information (ESI) to build the case and pinpoint key pieces of evidence. Unlike other eDiscovery solutions where you may need to sacrifice interface for functionality or vice versa, Casepoint provides a clean and intuitive interface with a depth of functionality (see **Error! Reference source not found.**) including analytics, visualization, and artificial intelligence



Figure 1 – Casepoint’s platform provides a unified SaaS environment to support the discovery needs of the WVOT

As outlined in Table 1 below, Casepoint brings several benefits to the WVOT including:

Table 1 - Casepoint's robust features bring value and benefits to the Office of Technology

Casepoint Features	Benefits to the WVOT
 Feature Rich, Scalable, & Customizable Platform Casepoint is a unified eDiscovery platform with robust functionality that is architected for speed and scalability. Casepoint can manage large volumes of data and support 600+ file types while maintaining fast processing speeds.	 Smarter eDiscovery By leveraging Casepoint's robust and scalable platform, the WVOT will realize improved eDiscovery through: <ul style="list-style-type: none"> - Streamlined data processing with fast processing speeds - Unified platform to seamlessly support end-to-end eDiscovery workflow - Intuitive interface, powerful analytics and artificial intelligence that allow users to quickly view, search, and tag ESI
 Purposeful Innovation As an independently owned and funded company, Casepoint has the flexibility to leverage the latest technology to drive efficiency in eDiscovery. Casepoint's innovation is evidenced through our early adoption of technologies like cloud, TAR, artificial intelligence, and advanced analytics.	 State-of-the-Art Technology is within Reach In addition to many of the aforementioned benefits, the WVOT will have increased ability to: <ul style="list-style-type: none"> - Support the continuously expanding data sources for discovery - Access the latest technology innovations to increase staffs' ability to conduct discovery
 Low Cost Casepoint is a SaaS platform with highly competitive and flexible pricing to meet WVOT's budget constraints. The entire Casepoint platform is available to an unlimited number of users at one simple price. System operations, maintenance and enhancements are included at no additional cost.	 Cost-Efficiency while Maintaining Quality Analytics & Service The WVOT will realize a lower total cost of ownership because no infrastructure or additional labor are required to support Casepoint.

1.1 About Casepoint

Casepoint is a dynamic team of legal, technology, and business professionals who understand case management and e-Discovery end-to-end. Casepoint empowers government agencies, leading law firms, and multinational corporations with a powerful, secure web-based platform that is cutting-edge and easy to use. Casepoint is used by thousands of attorneys, paralegals, and litigation support professionals around the world. Attorneys need to evaluate information about each case and make timely strategic decisions. Casepoint makes that happen quickly, defensibly, and cost-effectively. Simply put, Casepoint is smarter legal working.

Casepoint was established in 2008 and is unique in that we are solely owned, funded, and distributed, giving us full autonomy to deliver continuous innovation to our clients as part of our no cost upgrades. We highly value client feedback and suggestions and often incorporate client enhancement suggestions into our processes, procedures, and platform. In addition, we have a dedicated Public Sector division that is led by a team with over 25 years of experience working with Government agencies. We understand the sensitive contracting and security requirements of Government agencies and have developed a project approach that consistently delivers successful Casepoint implementations and high-quality services.

Likewise, Casepoint has experience working with Government agencies, including California Department of Business Oversight, US Courts, National Credit Union Administration, and the Connecticut Office of the Attorney General.

2 Qualifications & Requirements

Table 2 - Casepoint meets WVOT's required qualifications

Qualification	Casepoint Response
(3.1) The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section 9.3.1.12 - Remote Access requirements. (3.1.1) IRS 1075, Section 9.3.1.12 states that "FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore -outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore."	<p>Secure authorized access is paramount for Casepoint. Casepoint's user authentication model is governed by role-based security access rights based on case-level security, document-level security, and field-level security. Administrators can define the roles at the most granular level, including access to fields, tagging panels, screens, files/documents, menu options and folders, to name just a few. There are thousands of permission combinations that can be configured per Casepoint role and there can be unlimited roles associated per matter.</p> <p>In addition, Casepoint can whitelist designated IP addresses to limit and control access to only trusted users.</p>

Table 3 - Casepoint meets and exceeds WVOT's mandatory contract services requirements

Mandatory Requirements	Response
(4.1.1.1) The Vendor must provide an e-Discovery System that is cloud based (Software as a Service Model).	<p>Casepoint is a cloud-based SaaS platform with highly competitive and flexible pricing to meet the Office of Technology's budget constraints.</p> <p>Casepoint is browser, device, and platform agnostic. Casepoint can be accessed 24 hours/7 days a week from all standard web browsers that support TLS 1.1 or TLS 1.2 and from any internet-connected computer including most mobile devices (tablets including iPads and smart phones) without additional plug-ins. A user has full access to Casepoint whether they are utilizing Internet Explorer on a Windows machine, Safari or Firefox on a Mac, Google Chrome on a Chromebook or tablet.</p>
(4.1.1.2) The Vendor must provide an e-Discovery System with an unlimited user seats for a minimum of 12 months from date of award.	The entire Casepoint platform is available to an unlimited number of users at one simple price. System operations, maintenance, and enhancements are included at no additional cost.
(4.1.1.3.1) A system that has two factor authentication access.	Multi-factor authentication is supported by Casepoint for all internet facing access devices and websites. We have a defined set of password complexity requirements in addition to multifactor authentication that can be set to common authentication systems like Google Authenticator, Microsoft Authenticator, Duo Mobile, and others.

<p>(4.1.1.3.2) A system that allows the Agency to have 100% data input automation. The Vendor must not have access to Agency owned data.</p>	<p>Casepoint eDiscovery is designed to be self-service. As described in section 3.1.1 below, Casepoint eDiscovery offers the ability for the Agency to upload, ingest, and process directly in Casepoint eDiscovery. Thus, the Agency will have 100% data input automation.</p> <p>Casepoint's organizational security policies, including information security, data, and privacy policies, requires that access to Casepoint assets, including assets hosting client data, will be granted based on business justification, with the asset owner's authorization and limited access based on "need-to-know" and "least-privilege" principles.</p> <p>Note: As defined in the Software as a Service Addendum, Casepoint will have access to Agency data for the sole purposes of managing the Casepoint application and databases and responding to technical support and service requests.</p>
<p>(4.1.1.3.3) A system that provides 256-bit encryption to the data when at rest and in transit.</p>	<p>Casepoint uses FIPS 140-2 compliant algorithms such as AES256. Our storage systems use AES-256 encryption, and data in transit is encrypted using TLS1.2 with AES256. All media drives are encrypted with military grade encryptions. Also, Casepoint backups are encrypted with AES-256 encryption.</p>
<p>(4.1.1.3.4) A system that scans files for viruses.</p>	<p>Casepoint scans for viruses at ingestion as processing begins for native data. For processed data, Casepoint scans before loading to protect our servers from viruses.</p>
<p>(4.1.1.3.5) A system that allows for load file import and export</p>	<p>Casepoint supports 600+ file types including Microsoft Office and related formats, Exchange, SharePoint, Skype, commadelimited, EDRM XML, and Concordance load files Casepoint's processing engine automates the entire processing workflow - from ingestion and container identification to text and metadata extraction. Casepoint allows for productions in native, PDF and TIFF formats. Data can also be exported to industry standard load file formats, including CSV files, Summation Load files, Concordance Load files, Generic Load files and EDRM XML Load files.</p>
<p>(4.1.1.4.1) Support by telephone, online, in-app, and email 24 hours a day, 7 days a week, 365 days a year for troubleshooting technical issues.</p>	<p>Casepoint's official business hours are Monday through Friday 8am to 9pm ET. Outside of those hours, we will have a team on standby to provide technical support. Casepoint will provide Tier 1 Support (basic how to questions, e.g., how do I login, how do I find a document, how do a run a simple search, where is certain functionality located within the app, etc) for the first 90 days after contract award. Tier 3 Support (Bug Fixes) are provided for the life of the contract. Tier 2 Support (assistance performing functions in Casepoint) is considered a billable service and, based on our understanding, is not included in the scope of this contract.</p>

(4.1.1.4.2) A response time of a minimum of one (1) day to request for technical support.	Casepoint's technical response times for technical support requests depends on the issue severity, At a minimum, Casepoint will respond within one business day to requests for technical support.
(4.1.1.4.3) Access to knowledgebase, technical documentation, and online support resources.	Casepoint has developed a robust, comprehensive online Help Center that is accessible directly from Casepoint. The Help Center provides detailed information about all Casepoint functionality including step-by-step processes for how to perform various functions. The Help Center is easy to use, searchable and links users to related functionality. Casepoint users will find the user support and the Help Center as great supplements to the training sessions.

3 Casepoint eDiscovery

As a unified eDiscovery platform, Casepoint has its own powerful data processing engine built-in with the capability to access, transform, and control over 600+ file types. Data flows in Casepoint from one phase of the eDiscovery process to the next without concern for data loss.



Figure 2 - Casepoint handles all eDiscovery needs from input to output

And Casepoint is highly configurable, so workspaces, workflows, and templates can be set up to meet the unique needs of each custom case. Thus, giving *you* complete autonomy to

add workspaces to the system, add users to the organization and assign them to workspaces and roles, as well as, build customize workspaces and add templates to expedite case needs for increased efficiencies.

Casepoint eDiscovery is a fully functional review and production platform that is fast, powerful, and easy-to-use. With Casepoint eDiscovery, the WVOT will find a user-friendly platform provides a depth of functionalities including that provides self-service data ingestion and processing, analytics, visualization, artificial intelligence, advanced search functions, document review, tagging, and production. The sections below provide more details about functions and features available in Casepoint eDiscovery.

3.1.1 Data Ingestion and Processing

Casepoint eDiscovery's processing engine automates the entire processing workflow - from ingestion and container identification to text and metadata extraction. The system identifies anomalous files during processing and provides an exception list of files for review by the case team. Data is loaded into Casepoint eDiscovery for ingestion and cataloguing. Once data is catalogued, it is de-duplicated, de-NISTed, and pre-processed for loading into our review platform. The entire process of preparing files for review is tracked by Casepoint and its internal chain of custody system for accurate and complete data processing.

We offer the flexibility of allowing our clients to self-upload and process their data. The processing wizard (see Figure 3 below) guides an administrator through file uploads, processing requirements, custodian assignment, deduplication, and promotion to the review environment. Processing templates can be created to preselect common options for case types.

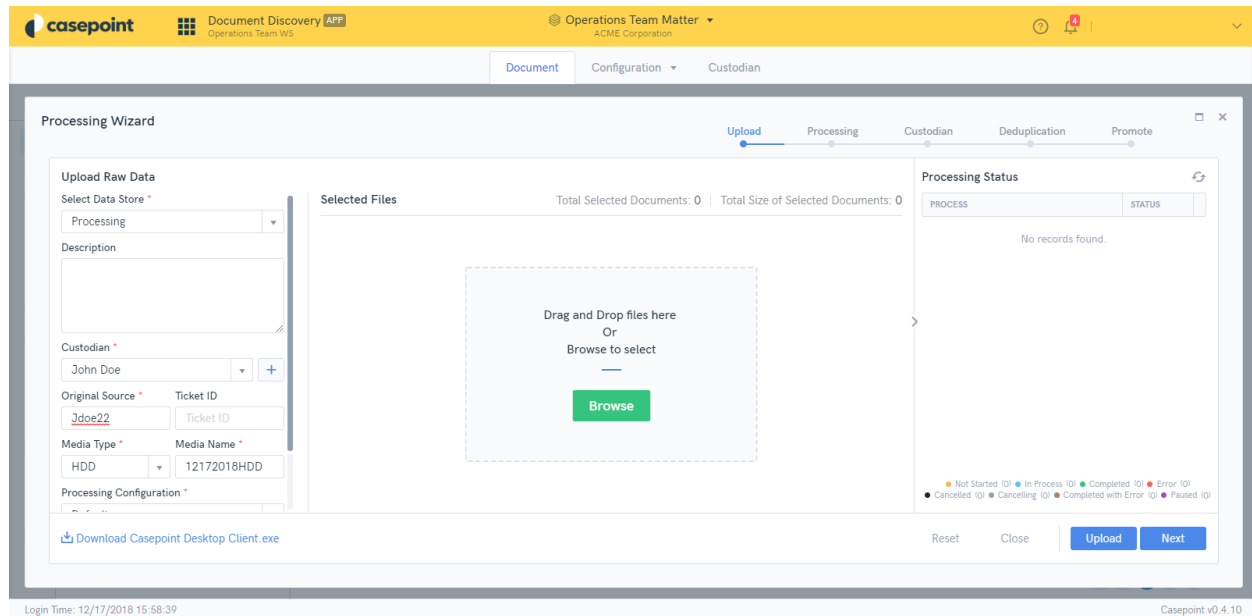


Figure 3 - Casepoint's processing wizard guides the administrator through data ingestion and processing

You can also perform OCR (Optical Character Recognition) and extract text from any image file format during processing and create or update a database index at anytime

3.1.2 Document Review

Casepoint eDiscovery is able to organize and segregate documents in many ways, including but not limited to, by any metadata field, tag, custom field, word search, or string search. Once organized and segregated, these documents can be saved into customizable folders accessible by permission at the case, group, and user level.

Casepoint eDiscovery has a batching tool that can be used to assign documents for review and track the status of document review. Casepoint doesn't limit the number of batches you can have for a case. Review batches can be organized by review phase. A phase can also be referred to as a review project (or a sub-project) or a batch set. Review batches can be assigned to a review team or to an individual. A reviewer can accept a batch and check it out to lock the batch for review. A reviewer can also share a batch or files in a batch with another user. Once all documents in a batch have been reviewed the status of the review batch is updated to complete.

Advanced Search

Casepoint eDiscovery has powerful search features that not only allow basic searching but also improve upon search criteria and ensure that you are searching effectively. The search functionality within Casepoint eDiscovery (see Figure 4Error! Reference source not found.) also allows you to explicitly include the family, e.g., an email (the parent) with

attachments (the children), in the search results. Casepoint maintains an audit of all searches and allows you to save the search criteria and search results.

Additionally, Casepoint eDiscovery has search related tools to validate each search term. For example, Casepoint eDiscovery provides synonym analysis, search term hit counts, fuzzy searching and stem searching to help determine that each search term selected is defensible. Casepoint eDiscovery's term analyzer identifies variations of search terms selected for search. The term analyzer also provides the ability to view hit counts of work variations to ensure you have selected the most effective search terms possible. Casepoint eDiscovery also has a sampling feature to vet each search result by creating a random sample of the search results and supports approximate string match searching, concept searching and concept clustering, and relevance ranking.

Casepoint eDiscovery also supports keyword term highlighting, as well as persistent highlighting of search terms, words or phrases throughout the collection. Hit highlighting is also available to users in text and attachments, allowing users to navigate from hit to hit.

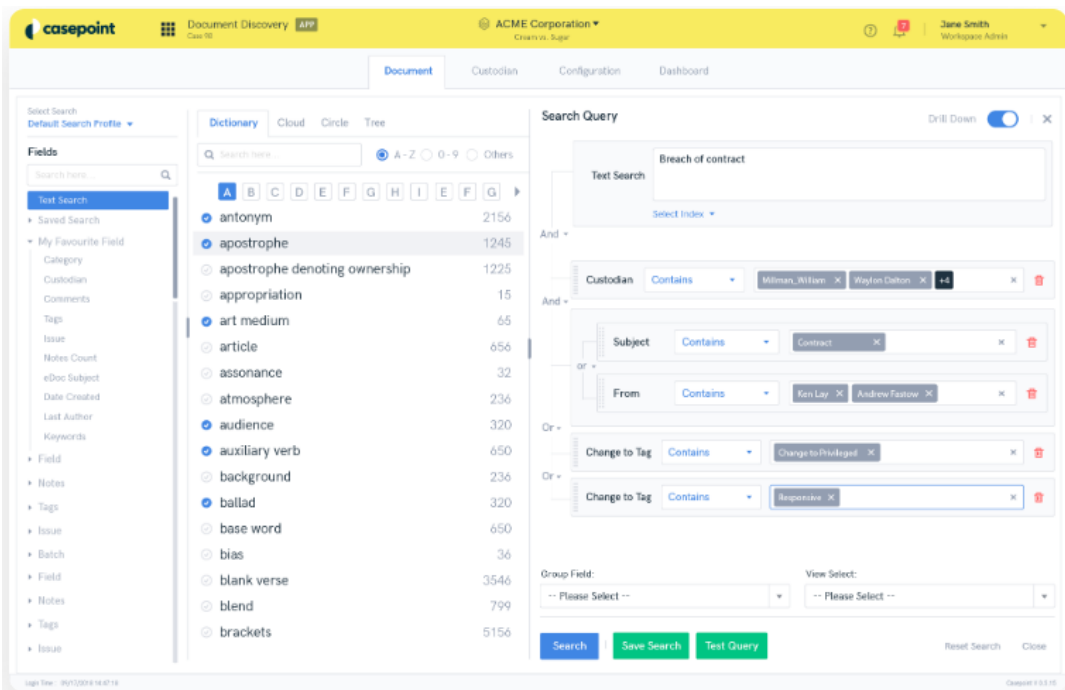


Figure 4 - Casepoint provides a search query wizard to build complex searches

Redactions

Casepoint eDiscovery has built-in annotation functionality that includes multiple redaction capabilities. Casepoint eDiscovery's redaction functionality allows authorized users to create multiple sets of redactions. These redactions can be turned on or turned off at any point so the document can be viewed with or without any version of the redactions. Redactions can also include specific text, such as, "Social Security Number" or "Birth Date."

Casepoint eDiscovery can even automatically find and redact photographs or specific faces in photos.

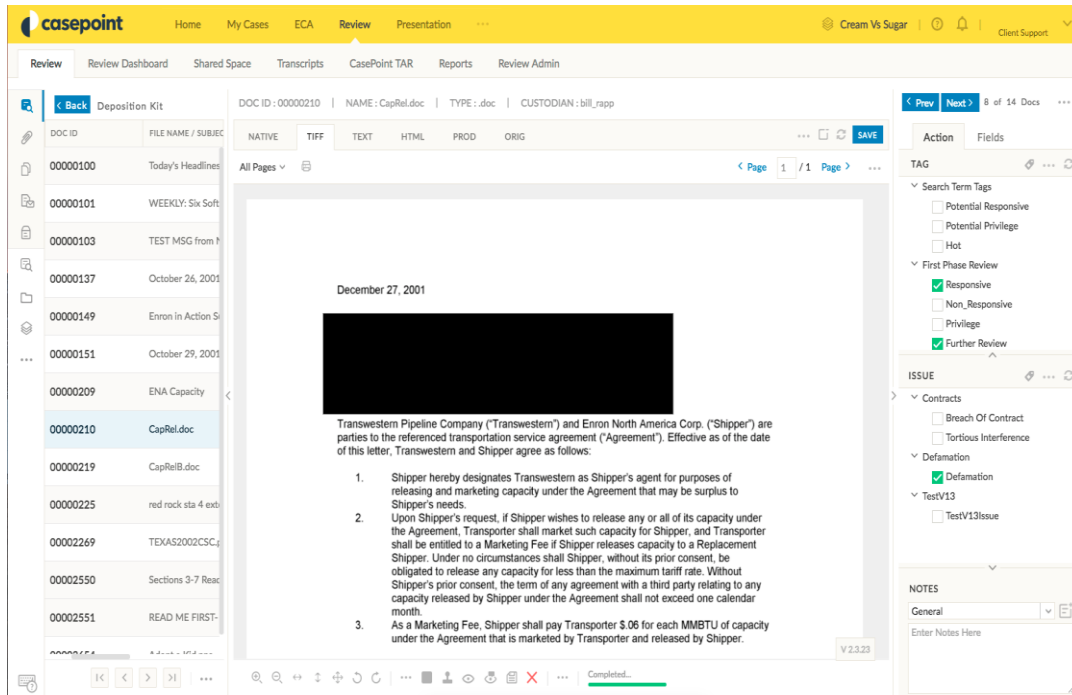


Figure 5 - Casepoint includes many redaction functionalities including TIFF document review redactions

Redactions are maintained as image coordinates within the database. At the time of production (export), redactions are burned into the production documents and the document is re-OCR'd to confirm that the underlying text is not included in any production. Additionally, reviewers can easily flag specific fields or data within records or define regular expressions to be redacted throughout all documentation.

3.1.3 Analytics and Artificial Intelligence

Casepoint eDiscovery's advanced artificial intelligence and analytics features, described below, are designed to help you quickly find key pieces of information and efficiently review large quantities of files.

Near Duplicate

Casepoint includes analytics for near-duplicate identification, comparison, and analysis of duplicate data. Redline, percentage similar, difference highlighting and side-by-side comparison views are functionalities that are standard features available in the Casepoint platform. With near duplicate and text similarity built right in, Casepoint has sophisticated tools to compare documents that are similar to other documents.

This feature goes far beyond a "tracked changes" document, and is able to show similar documents side by side highlighting differences between similar documents (see Figure 6

below). If you find a document that is relevant to your request, you will be able to easily find similar documents with a click of a button. The near duplicate feature allows for faster and more accurate reviews while reducing review effort.

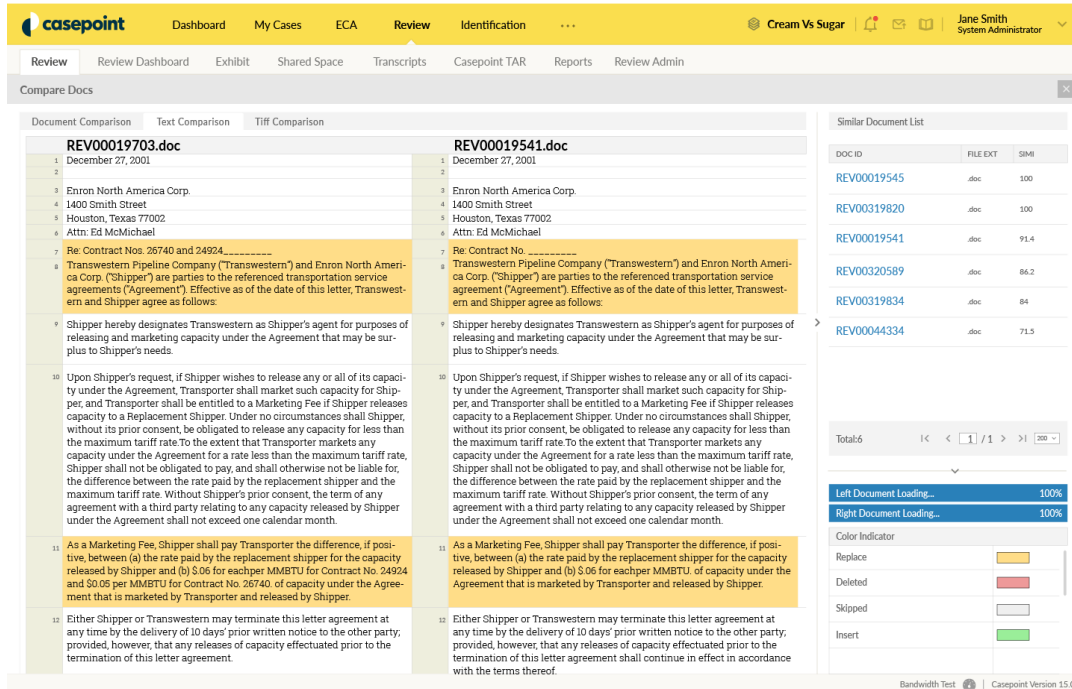


Figure 6 - Casepoint's DeNist, DeDupe, Near Similarity tool

Analytics Reporting

Casepoint eDiscovery gives you the option of analyzing data through visual representations including Word Clouds (see Figure 7), Timelines, Bubble Charts, and cluster Diagrams.

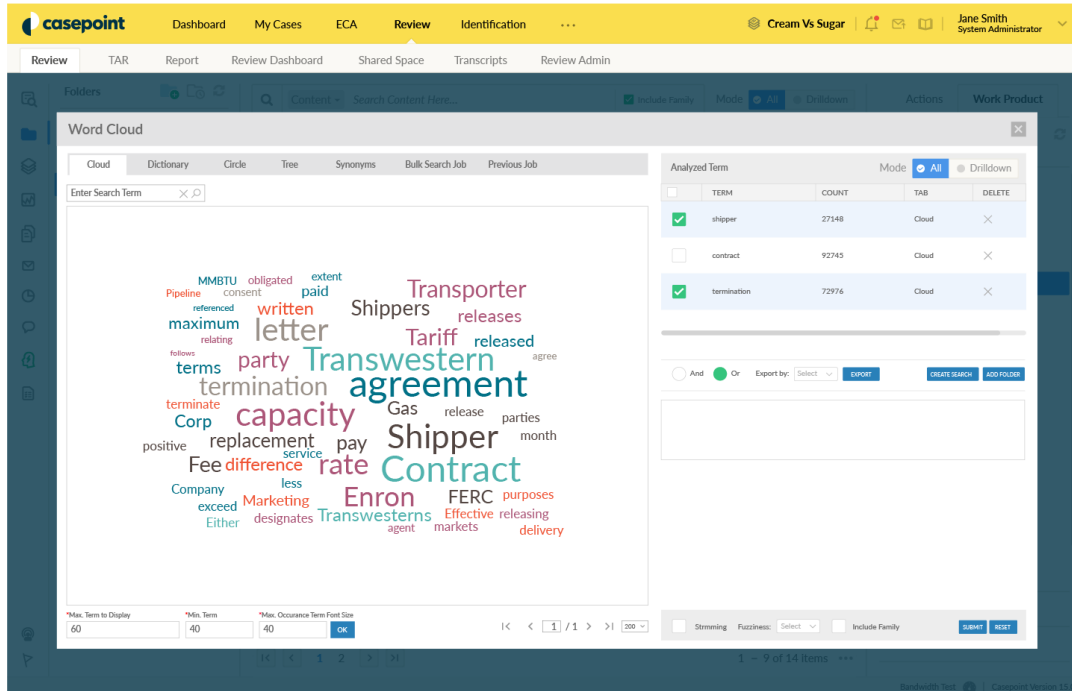


Figure 7 - Casepoint's data analysis and visualization tools includes a word cloud which displays the most commonly used words contained throughout the documents

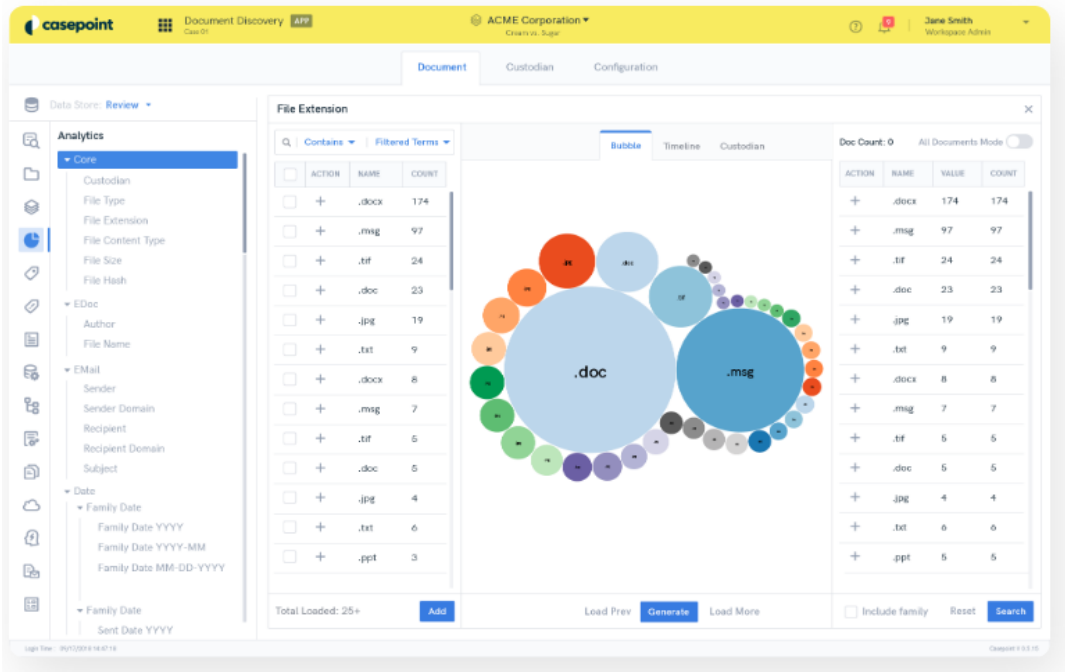


Figure 8 - Casepoint includes built-in advanced analytic tools that provide the user with a variety of ways to visualize data

Email Analytics

Casepoint includes email threading functionality and also performs email thread analysis. Casepoint's email threading feature clusters email communications using the Email Subject and the threads with the same Email Subject. Email threading review allows a user to group email communications and review documents by electronically mapping communication flow. Figure 9 shows how you can easily view email threads and branches. You can visually select any part of the thread to view and even tag.

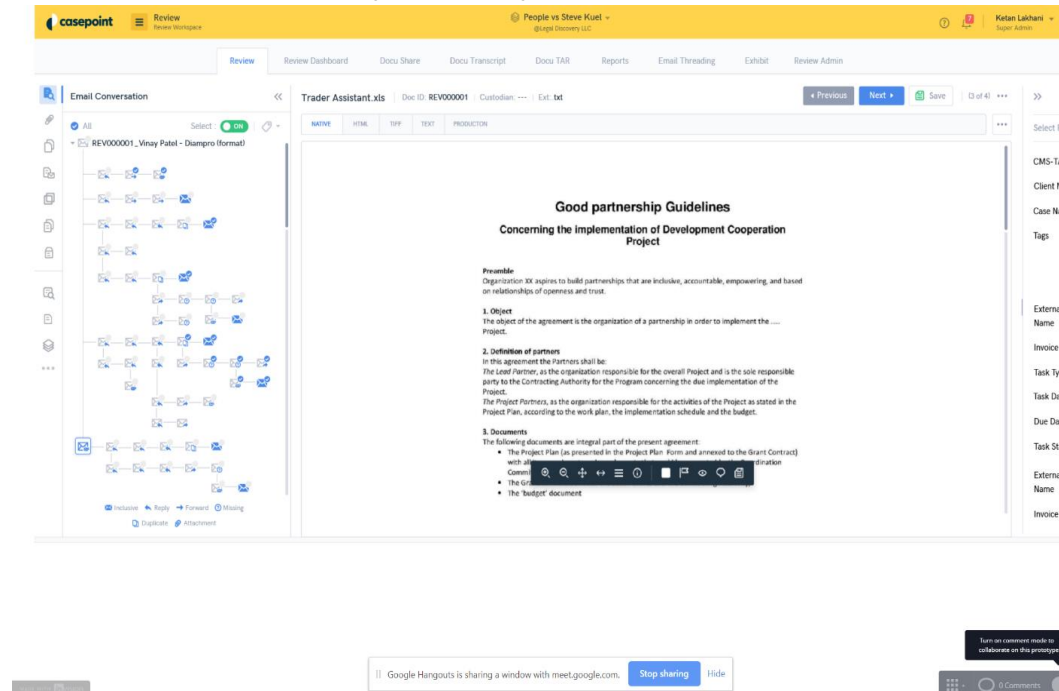


Figure 9 - Casepoint's email threading allows you to visualize threads and branches

Casepoint identifies the most inclusive email so you don't need to review all emails in the thread. In addition, emails are maintained as separate files so they can be searched and sorted on individually.

Email threading also displays historical trail of emails exchanged between a specific sender and receiver, including any missing emails that may have been deleted or removed. Any deleted or removed messages are designated as missing in the email thread tree. From the email threading view, a reviewer can see who, when, and how frequently the subjects interacted with each other and/or with others.



Figure 10 – Casepoint provides visualizations to show links between email communications

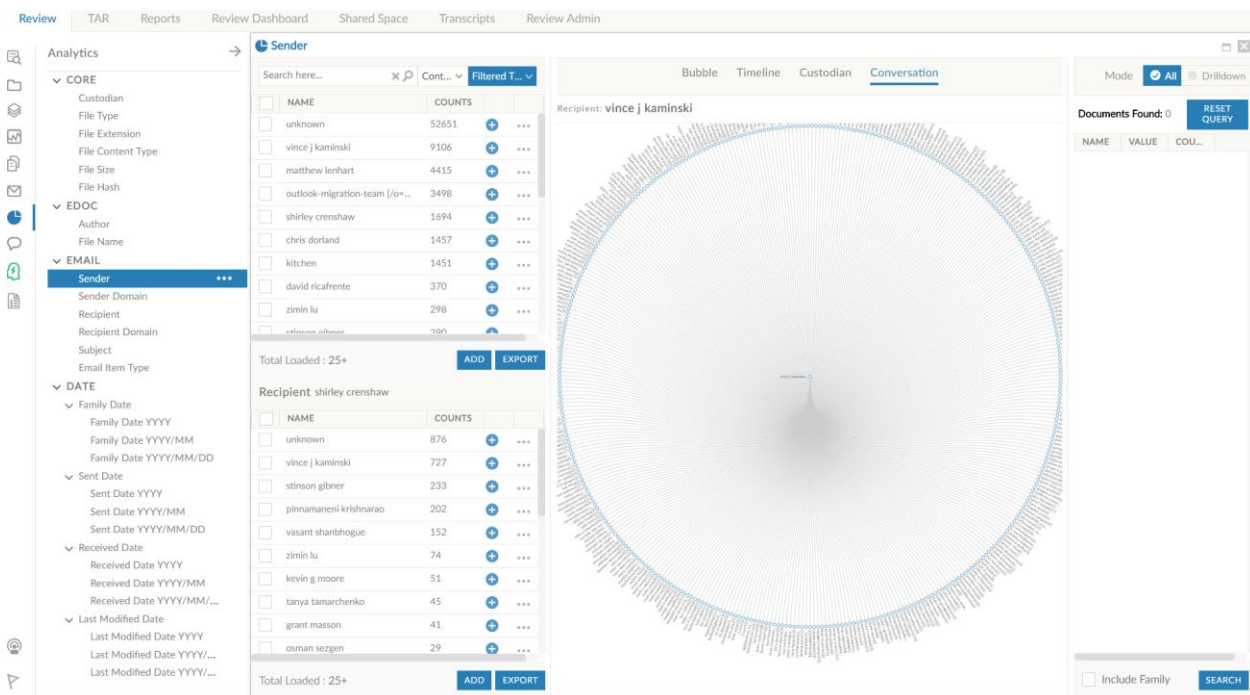


Figure 11 - Casepoint's Graphical Email Threading View

CaseAssist

CaseAssist revolutionizes the entire workflow of eDiscovery matters and internal investigations by proactively presenting relevant information to reviewers, attorneys and investigators and enabling them to focus on the legal arguments, storylines, and whether to pursue the matter at hand. Instead of laboriously running complex search terms, analyzing static randomized samples or reviewing predefined batches of documents,

team members can provide discrete pieces of information about a case such as people, dates, key words, and documents, and CaseAssist will find key documents relating to that information within moments.

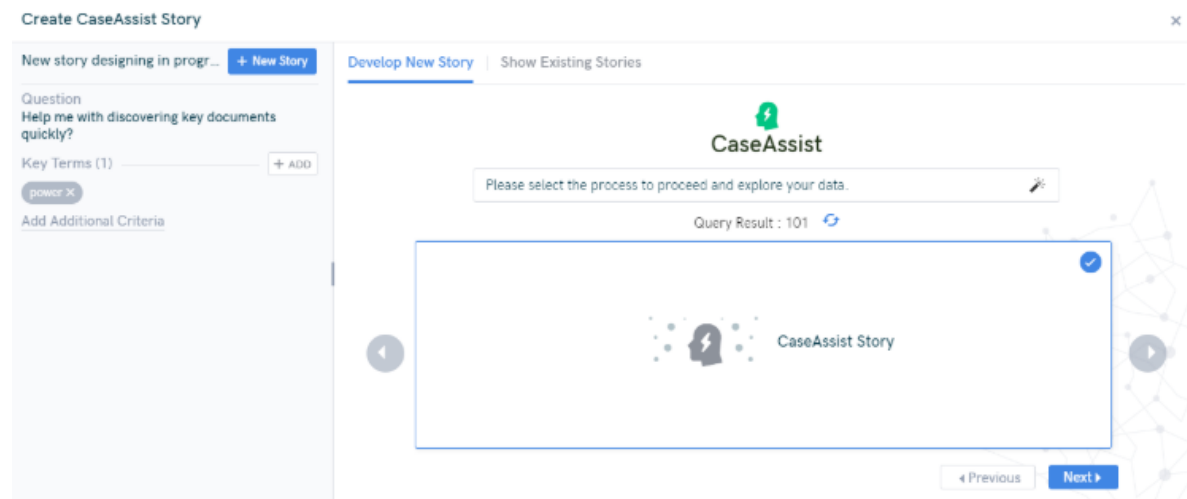


Figure 12 – CaseAssist

Easy to visualize and navigate, CaseAssist is a significant improvement to advanced search and analytics and provides access to the information in an intuitive way. CaseAssist also learns from documents you tag and suggests additional documents for analysis. It can be fully controlled by the user without the need for a project manager to oversee and facilitate the process. CaseAssist is an ideal technology to find information quickly without the need for high technical skill.

TAR

Artificial Intelligence, Technology Assisted Review (TAR) and Computer Assisted Learning technology are included in Casepoint eDiscovery at no extra charge. Team members have the ability to independently setup and create iterative TAR sessions and CaseAssist stories. Casepoint's TAR 1.0 allows a traditional TAR review whereby an experienced attorney/subject matter expert is able to review and train sample sets in multiple iterations based on the accuracy and f-measure score levels desired.

3.1.4 Productions

Casepoint's production capabilities are wizard driven and include all industry standard file formats for export. Casepoint supports mixed productions with native files, slip sheets, placeholders and image files. Production templates can be built to streamline and speed up production outputs.

Once data has been reviewed for responsiveness, privilege, and other issue coding, data that has been selected for production will be produced from the Casepoint eDiscovery. We

offer the flexibility of allowing designated users the ability to create their own productions at any time.

The production/export wizard guides an administrator through the configuration, quality control, preparation, and validation steps for a production. Production templates can be created to pre-select common options across cases.

3.1.5 User Access and Security

The Casepoint platform is designed to support the unique workflows of financial cases and can help securely handle the nuances associated with protecting sensitive data while the case progresses.

Roles and Permissions

Casepoint's user authentication model is governed by role-based security access rights based on case-level security, document-level security, and field-level security. Casepoint access is locked down at the case/matter level utilizing a comprehensive security matrix for roles and access. Administrators can define the roles at the most granular level, including access to fields, tagging panels, screens, files/documents, menu options and folders, to name just a few. There are thousands of permission combinations that can be configured per role and there can be unlimited roles associated per matter.

Security

Casepoint is very focused on security and we are currently providing a secure environment for our Government agency's highly sensitive data. For the US Courts Defenders Services Office, we host and manage data that is often covered by a protective order and includes sensitive information like personal identifiers of informants and defendants who are cooperators against other potentially violent defendants, financial documents, and patient records.

At the platform level, we have several security controls in place and received security certifications including:

- SOC II Type 2 Certification
- ISO 27001:2013 Assessment
- FIPS 140-2 Controls
- NIST 800-53 Controls

4 Previous Casepoint Implementations

As a company, Casepoint is experienced in the evolution of eDiscovery technology from the early days to present. Many on our team were early pioneers in eDiscovery, enabling our company to appreciate the intricacies of the industry and individual technologies including advanced analytics and predictive coding.

Casepoint's web-hosted review platform has been implemented for 159 clients and used for over 1500 matters. Casepoint delivers eDiscovery and litigation support services to:

- Government Agencies
- State and Local Agencies
- Law Firms for matters involving verticals including FCPA, finance, construction, pharma, IP, white collar and criminal litigation
- Construction, banking and insurance corporations

We currently have 15,000+ logins with users in USA, Canada, EU, Japan, South Korea, and India.

Casepoint has experience with a wide variety and large volumes of ESI – some of our recent matters include:

- A complex corporate matter – 22TB of data, mounted, culled, and processed in a record 4-day period with “on-the-fly” language translations
- A major antitrust litigation – 8TB of data, 15M documents, multiple counsel, multiple time zones, and multiple languages
- A large DOJ investigation – 12TB of data, joint defense matter
- A high-profile congressional inquiry – cloud email collection with over 100 custodians

In Table 4 **Error! Reference source not found.** below, we provide examples of some of our recent and relevant government experience to showcase our depth and breadth of relevant experience. These examples also highlight how Casepoint can support government divisions for various legal and discovery matters.

Table 4 - Casepoint's Depth and Breadth of Relevant Experience

Client	Demonstrated Services
U.S. Courts, Defender Services Office The US Courts Defenders Services Office (DSO) is responsible for the administration and support of the Defender Services Program. The Defenders Services Program provides defense resources as part of the Criminal Justice Act (CJA) to any person financially unable to obtain adequate representation.	Casepoint is working hand-in-hand with the DSO Administrative Office to deploy Casepoint across 79 DSOs covering 94 districts. This includes outreach, demonstrations, training, and user support so users become comfortable with the Casepoint Platform and quickly see the benefit of Casepoint's powerful e-Discovery capabilities. We work with each DSO to understand their requirements and configure Casepoint to meet their specific needs. In addition, we have made customizations to Casepoint to resolve complex data challenges

Client	Demonstrated Services
	like mapping audio video files from police encounters to transcript line items.
National Credit Union Administration The National Credit Union Administration (NCUA) The mission of the NCUA provides, through regulation and, a safe and sound credit union system, which promotes confidence in the national system of cooperative credit.	Casepoint provided full e-Discovery support and services including onsite data collections, project management, consulting, and advanced analytics to assist NCUA's litigation support team to identify the smallest, most-relevant data for the case quickly and cost-effectively. With training and guidance from Casepoint's support team combined with Casepoint's advanced features, NCUA was able to quickly and efficiently produce data within the deadline.
California Department of Business Oversight (DBO) The DBO protects consumers and oversees financial service providers and products. The DBO supervises the operations of state-licensed financial institutions, including banks, credit unions and money transmitters. Additionally, the DBO licenses and regulates a variety of financial service providers, including securities brokers and dealers, investment advisers, payday lenders and other consumer finance lenders.	Casepoint worked with DBO to complete an enterprise-wide rollout of Casepoint. This included several basic and advanced onsite training sessions to 100+ users. Casepoint is used across DBO to support over 30 matters. DBO is leveraging the basic and advanced features of Casepoint including basic and advanced search, coding, annotation, redactions, and TAR.
State of Connecticut, Office of Attorney General The Attorney General is the chief civil legal officer of the State. The Office of the Attorney General was officially established in 1897. The Connecticut Constitution and General Statutes authorize the Attorney General to represent the interests of the people of the State of Connecticut in all civil legal matters involving the state to protect the public interest, and to serve as legal counsel to all state agencies.	Casepoint provides a comprehensive cloud-based solution to serve the litigation needs of the State of Connecticut including 15 departments and offices across Connecticut State Agencies. Specifically, Casepoint is used to support efforts across tort cases, employment issues, class action lawsuits and FOIA requests. Connecticut's local administrators leverages Casepoint's user and account management capabilities to quick setup cases and manage templates and users at the account and case level.



Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 - Info Technology

Proc Folder: 619426

Doc Description: e-Discovery Software as a Service (OT19141)

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2019-12-13	2020-01-02 13:30:00	CRFQ 0210 ISC2000000011	1

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON

WV 25305

US

VENDOR

Vendor Name, Address and Telephone Number:

Casepoint, LLC
7900 Tysons One Place
Suite 680
Tysons VA 22102

FOR INFORMATION CONTACT THE BUYER

Jessica S Chambers

(304) 558-0246

jessica.s.chambers@wv.gov

Signature X

FEIN #

300503533

DATE

12/19/2019

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION:

: The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Office of Technology to establish a contract for an e-Discovery software as a service. This software will be used for discovery in legal proceedings to process emails and other files. The software will facilitate keyword searching, document review, privilege report creation, data tagging and redaction prior to final report being released per the terms and conditions and specifications as attached.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Contract Services: e-Discovery System	100.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :

Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line

The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

*** Please note quantities listed are estimates only. Actual quantities may differ.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Opt Renewal Y2: Contract Services: e-Discovery System	100.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :

Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line

The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

Contract will be evaluated on all lines but only awarded on first year.

Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

*** Please note quantities listed are estimates only. Actual quantities may differ.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Opt Renewal Y3: Contract Services: e-Discovery System	100.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :

Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line

The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

Contract will be evaluated on all lines but only awarded on first year.

Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

*** Please note quantities listed are estimates only. Actual quantities may differ.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV25305 US	IS&C - CHIEF FINANCIAL OFFICER DEPARTMENT OF ADMINISTRATION BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV 25305 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Opt Renewal Y4: Contract Services: e-Discovery System	100.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description :

Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line

The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

Contract will be evaluated on all lines but only awarded on first year.

Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

*** Please note quantities listed are estimates only. Actual quantities may differ.

SCHEDULE OF EVENTS		
--------------------	--	--

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Technical Question Deadline	2019-12-23

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. REVIEW DOCUMENTS THOROUGHLY: The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. MANDATORY TERMS: The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. PREBID MEETING: The item identified below shall apply to this Solicitation.

☒ A pre-bid meeting will not be held prior to bid opening

☐ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in, but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting
Revised 11/14/2019

are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

4. VENDOR QUESTION DEADLINE: Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below in order to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted e-mails should have solicitation number in the subject line.

Question Submission Deadline: December 23, 2019 at 12:00 PM (EST)

Submit Questions to: Jessica Chambers

2019 Washington Street, East

Charleston, WV 25305

Fax: (304) 558-4115 (Vendors should not use this fax number for bid submission)

Email: Jessica.S.Chambers@wv.gov

5. VERBAL COMMUNICATION: Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

6. BID SUBMISSION: All bids must be submitted electronically through wvOASIS or signed and delivered by the Vendor to the Purchasing Division at the address listed below on or before the date and time of the bid opening. Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via e-mail. Acceptable delivery methods include electronic submission via wvOASIS, hand delivery, delivery by courier, or facsimile.

The bid delivery address is:

Department of Administration, Purchasing Division

2019 Washington Street East

Charleston, WV 25305-0130

A bid that is not submitted electronically through wvOASIS should contain the information listed below on the face of the envelope or the bid may be rejected by the Purchasing Division.:

SEALED BID:

BUYER: Jessica Chambers

SOLICITATION NO.: CRFQ ISC2000000011

BID OPENING DATE: 1/02/2020

BID OPENING TIME: 1:30 PM (EST)

FAX NUMBER: (304)558-3970

Revised 11/14/2019

The Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. Submission of a response to an Expression or Interest or Request for Proposal is not permitted in wvOASIS.

For Request For Proposal ("RFP") Responses Only: In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal plus _____ convenience copies of each to the Purchasing Division at the address shown above. Additionally, the Vendor should identify the bid type as either a technical or cost proposal on the face of each bid envelope submitted in response to a request for proposal as follows:

BID TYPE: (This only applies to CRFP)

☐ Technical

☐ Cost

7. BID OPENING: Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: January 2, 2020 at 1:30 PM (EST)

Bid Opening Location: Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

8. ADDENDUM ACKNOWLEDGEMENT: Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

9. BID FORMATTING: Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

10. ALTERNATE MODEL OR BRAND: Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the

equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

☐ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

11. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

12. COMMUNICATION LIMITATIONS: In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

13. REGISTRATION: Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the \$125 fee, if applicable.

14. UNIT PRICE: Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

15. PREFERENCE: Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and should include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at:

<http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf>.

15A. RECIPROCAL PREFERENCE: The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. A request form to help facilitate the request can be found at:

<http://www.state.wv.us/admin/purchase/vrc/Venpref.pdf>.

16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES: For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37(a)(7) and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the

Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

17. WAIVER OF MINOR IRREGULARITIES: The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.

18. ELECTRONIC FILE ACCESS RESTRICTIONS: Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires, and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

19. NON-RESPONSIBLE: The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform, or lacks the integrity and reliability to assure good-faith performance.”

20. ACCEPTANCE/REJECTION: The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b.”

21. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor’s entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled “confidential,” “proprietary,” “trade secret,” “private,” or labeled with any other claim against public disclosure of the documents, to include any “trade secrets” as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

22. INTERESTED PARTY DISCLOSURE: West Virginia Code § 6D-1-2 requires that the vendor submit to the Purchasing Division a disclosure of interested parties to the contract for all contracts with an actual or estimated value of at least \$1 Million. That disclosure must occur on the form prescribed and approved by the WV Ethics Commission prior to contract award. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

23. WITH THE BID REQUIREMENTS: In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of a Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or "Agencies" means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or "Proposal" means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or "Vendors" means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☒ **Term Contract**

Initial Contract Term: **Initial Contract Term:** This Contract becomes effective on _____ upon award _____ and extends for a period of one (1) year(s).

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____ days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that maintenance, monitoring, or warranty services will be provided for _____ year(s) thereafter.

☐ **One Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Other:** See attached.

4. NOTICE TO PROCEED: Vendor shall begin performance of this Contract immediately upon receiving notice to proceed unless otherwise instructed by the Agency. Unless otherwise specified, the fully executed Award Document will be considered notice to proceed.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☒ **Open End Contract:** Quantities listed in this Solicitation are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☒ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☐ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

☐ **One Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One Time Purchase contract.

7. REQUIRED DOCUMENTS: All of the items checked below must be provided to the Purchasing Division by the Vendor as specified below.

☐ **BID BOND (Construction Only):** Pursuant to the requirements contained in W. Va. Code § 5-22-1(c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. The bid bond must be submitted with the bid.

☐ **PERFORMANCE BOND:** The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contract award.

☐ **LABOR/MATERIAL PAYMENT BOND:** The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior to Contract award.

In lieu of the Bid Bond, Performance Bond, and Labor/Material Payment Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any certified check, cashier's check, or irrevocable letter of credit provided in lieu of a bond must be of the same amount and delivered on the same schedule as the bond it replaces. A letter of credit submitted in lieu of a performance and labor/material payment bond will only be allowed for projects under \$100,000. Personal or business checks are not acceptable. Notwithstanding the foregoing, West Virginia Code § 5-22-1 (d) mandates that a vendor provide a performance and labor/material payment bond for construction projects. Accordingly, substitutions for the performance and labor/material payment bonds for construction projects is not permitted.

☐ **MAINTENANCE BOND:** The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award.

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☐

☐

☐

☐

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below and must include the State as an additional insured on each policy prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed in this section.

Vendor must maintain:

☒ **Commercial General Liability Insurance** in at least an amount of: \$1,000,000.00 per occurrence.

☐ **Automobile Liability Insurance** in at least an amount of: _____ per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _____ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: _____ per occurrence.

☒ **Cyber Liability Insurance** in an amount of: \$1,000,000.00 per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: _____ per occurrence.

☐ **Aircraft Liability** in an amount of: _____ per occurrence.

☐☐☐☐

Notwithstanding anything contained in this section to the contrary, the Director of the Purchasing Division reserves the right to waive the requirement that the State be named as an additional insured on one or more of the Vendor's insurance policies if the Director finds that doing so is in the State's best interest.

9. WORKERS' COMPENSATION INSURANCE: The apparent successful Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. [Reserved]

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☐ _____ for _____

☐ Liquidated Damages Contained in the Specifications

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

14. PAYMENT IN ARREARS: Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices, in arrears.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

20. TIME: Time is of the essence with regard to all matters of time and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in <http://www.state.wv.us/admin/purchase/privacy/default.html>.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

34. VENDOR CERTIFICATIONS: By signing its bid or entering into this Contract, Vendor certifies (1) that its bid or offer was made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services; (2) that its bid or offer is in all respects fair and without collusion or fraud; (3) that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; and (4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein.

Vendor's signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency. The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

37. PURCHASING AFFIDAVIT: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State, Vendors are required to sign, notarize, and submit the Purchasing Affidavit to the Purchasing Division affirming under oath that it is not in default on any monetary obligation owed to the state or a political subdivision of the state.

38. ADDITIONAL AGENCY AND LOCAL GOVERNMENT USE: This Contract may be utilized by other agencies, spending units, and political subdivisions of the State of West Virginia; county, municipal, and other local government bodies; and school districts ("Other Government Entities"), provided that both the Other Government Entity and the Vendor agree. Any extension of this Contract to the aforementioned Other Government Entities must be on the same prices, terms, and conditions as those offered and agreed to in this Contract, provided that such extension is in compliance with the applicable laws, rules, and ordinances of the Other Government Entity. A refusal to extend this Contract to the Other Government Entities shall not impact or influence the award of this Contract in any manner.

39. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

40. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☐ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.requisitions@wv.gov.

41. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry.

After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the Director of the Division of Protective Services for purposes of verifying compliance with this provision. The State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.

Revised 11/14/2019

Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

42. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more of such operations, from steel made by the open hearth, basic oxygen, electric furnace, Bessemer or other steel making process. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:
- c. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
- d. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

43. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a

“substantial labor surplus area”, as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

44. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the vendor must submit to the Agency a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-award interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

45. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

2 Amy Hilbert, Vice President Public Sector
(Name, Title)
Amy Hilbert vice President Public Sector
(Printed Name and Title)
7900 Tysons One Place, Suite 680, Tysons VA 22102
(Address)
703-738-4408
(Phone Number) / (Fax Number)
ahilbert@casepoint.com
(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Casepoint, LLC
(Company)
Amy Hilbert, vice President Public Sector
(Authorized Signature) (Representative Name, Title)
Amy Hilbert, Vice President Public Sector
(Printed Name and Title of Authorized Representative)
12/19/19
(Date)
703-738-4408
(Phone Number) (Fax Number)

REQUEST FOR QUOTATION
e-Discovery Software as a Service

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Office of Technology to establish a contract for an e-Discovery software as a service. This software will be used for discovery in legal proceedings to process emails and other files. The software will facilitate keyword searching, document review, privilege report creation, data tagging and redaction prior to final report being released.
2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.
 - 2.1 **“Business Hours”** means Monday - Friday 8:00 AM to 5:00 PM EST excluding weekends and Federal and State holidays, which are as follows:
 - 2.1.1 New Year’s Day (January 1)
 - 2.1.2 Martin Luther King Day (Third Monday in January)
 - 2.1.3 President’s Day (Third Monday in February)
 - 2.1.4 Memorial Day (Last Monday in May)
 - 2.1.5 West Virginia Day (June 20)
 - 2.1.6 Independence Day (July 4)
 - 2.1.7 Labor Day (First Monday in September)
 - 2.1.8 Columbus Day (Second Monday in October)
 - 2.1.9 Veterans Day (November 11)
 - 2.1.10 Thanksgiving (Fourth Thursday in November)
 - 2.1.11 Day After Thanksgiving (Fourth Friday in November)
 - 2.1.12 Christmas Day (December 25)
 - 2.2 **“Contract Services”** means e-Discovery system as more fully described in these specifications.
 - 2.3 **“Pricing Page”** means the pages, contained wvOASIS or attached hereto as Exhibit A, upon which Vendor should list its proposed price for the Contract Services.
 - 2.4 **“Solicitation”** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.
3. **QUALIFICATIONS:** Vendor, or Vendor’s staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:
 - 3.1. The Vendor must provide a product that is a ‘leader’ according to Gartner’s Magic Quadrant for e-discovery software as a service and must provide proof of this certification upon request.
 - 3.2. The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section 9.3.1.12 – Remote Access requirements.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

- 3.2.1. IRS 1075, Section 9.3.1.12 states that *“FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore - outside of the United States territories, embassies, or military installations. Further, FTI may not be received, processed, stored, transmitted, or disposed of by IT systems located offshore.”*

4. MANDATORY REQUIREMENTS:

4.1 Mandatory Contract Services Requirements and Deliverables: Contract Services must meet or exceed the mandatory requirements listed below.

4.1.1 Contract Services – e-Discovery System

- 4.1.1.1 The Vendor must provide an e-Discovery System that is cloud based (Software as a Service Model).
- 4.1.1.2 The Vendor must provide an e-Discovery System with an unlimited user seats for a minimum of 12 months from date of award.
- 4.1.1.3 The Vendor must provide an e-Discovery System that features the following:
- 4.1.1.3.1 A system that has two factor authentication access.
- 4.1.1.3.2 A system that allows the Agency to have 100% data input automation. The Vendor must not have access to Agency owned data.
- 4.1.1.3.3 A system that provides 256-bit encryption to the data when at rest and in transit.
- 4.1.1.3.4 A system that scans files for viruses.
- 4.1.1.3.5 A system that allows for load file import and export.
- 4.1.1.4 The Vendor must provide support that includes the following:
- 4.1.1.4.1 Support by telephone, online, in-app, and email 24 hours a day, 7 days a week, 365 days a year for troubleshooting technical issues

REQUEST FOR QUOTATION
e-Discovery Software as a Service

4.1.1.4.2 A response time of a minimum of one (1) day to request for technical support.

4.1.1.4.3 Access to knowledgebase, technical documentation, and online support resources.

4.1.1.5 Vendor will include in their bid the cost of optional Annual renewals for years 2, 3, and 4. These optional Annual renewals will be initiated on Agency request authorized under the authority of the Purchasing Division.

4.1.2 Software as a Service Addendum

4.1.2.1 Vendor must sign the attached Software as a Service Addendum prior to award.

5. CONTRACT AWARD:

5.1 Contract Award: The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the Vendor that provides the Contract Services meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

Contract will be evaluated on all lines but only awarded on first year.

Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

5.2 Pricing Page: Vendor should complete the Commodity Lines in Oasis, which will be used as the referenced Pricing Page by providing the unit cost per Gigabyte (GB). The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line 1. The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

The Pricing Page contain a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

Vendor should provide with their bid a copy of any and all Software Terms and Conditions or licenses that the State of West Virginia or the Agency will have to agree to or accept as a part of this solicitation. This information will be required before contract is issued.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

Vendor should include a copy of any Maintenance Terms and Conditions or Licenses that the State of West Virginia or the Agency will be required to agree to and accept as a part of this solicitation. This information will be required before contract is issued.

Vendor should type or electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document.

6. **PERFORMANCE:** Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.
7. **PAYMENT:** Agency shall pay a flat fee, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.
8. **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.
9. **FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:
 - 9.1. Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
 - 9.2. Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.
 - 9.3. Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
 - 9.4. Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
 - 9.5. Vendor shall inform all staff of Agency's security protocol and procedures.

10. VENDOR DEFAULT:

- 10.1. The following shall be considered a vendor default under this Contract.

- 10.1.1. Failure to perform Contract Services in accordance with the requirements contained herein.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

- 10.1.2. Failure to comply with other specifications and requirements contained herein.
- 10.1.3. Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.
- 10.1.4. Failure to remedy deficient performance upon request.
- 10.2. The following remedies shall be available to Agency upon default.
 - 10.2.1. Immediate cancellation of the Contract.
 - 10.2.2. Immediate cancellation of one or more release orders issued under this Contract.
 - 10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS:

- 11.1. **Contract Manager:** During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager:	Amy Hilbert
Telephone Number:	703-738-4408
Fax Number:	
Email Address:	ahilbert@casepoint.com

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
- c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
- d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
- e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
- g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
- i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
 - 10 days after the effective date of termination, if the termination is in accordance with the contract period
 - 30 days after the effective date of termination, if the termination is for convenience
 - 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

- Access and use the service for its business purposes;
- For SaaS, use underlying software as embodied or used in the service; and
- View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency: _____

Name of Vendor: Casepoint2LC

Signature: _____

Signature: [Handwritten Signature]

Title: _____

Date: _____

Title: Vice President, public sector

Date: 12/19/2019

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency: _____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
Yes ☐
No ☐
2. If yes to #1, does the restricted information include personal data?
Yes ☐
No ☐
3. If yes to #1, does the restricted information include non-public data?
Yes ☐
No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes ☐
No ☐
5. Provide name and email address for the Department privacy officer:

Name: _____

Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

Name: _____

Email address: _____

Phone Number: _____

West Virginia Ethics Commission



Disclosure of Interested Parties to Contracts

Pursuant to *W. Va. Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of \$1 million or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

"Business entity" means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation, but does not include publicly traded companies listed on a national or international stock exchange.

"Interested party" or *"Interested parties"* means:

- (1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
- (2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
- (3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

"State agency" means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of *W. Va. Code* § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: www.ethics.wv.gov.

West Virginia Ethics Commission
Disclosure of Interested Parties to Contracts

(Required by W. Va. Code § 6D-1-2)

Name of Contracting Business Entity: Casepoint LLC Address: 7900 Tysons One Place
Suite 680 Tysons VA 22102

Name of Authorized Agent: _____ Address: _____

Contract Number: _____ Contract Description: _____

Governmental agency awarding contract: State of West Virginia Purchasing Division

☐ Check here if this is a Supplemental Disclosure

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below (attach additional pages if necessary):

1. Subcontractors or other entities performing work or service under the Contract

☒ Check here if none, otherwise list entity/individual names below.

2. Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)

☒ Check here if none, otherwise list entity/individual names below.

3. Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)

☒ Check here if none, otherwise list entity/individual names below.

Signature: [Signature]

Date Signed: 12/19/2019

Notary Verification

State of Virginia, County of Fairfax

I, Jovie Gentile, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 19th day of December, 2019.

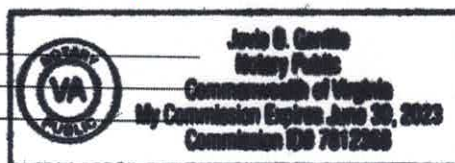
[Signature]
Notary Public's Signature

To be completed by State Agency:

Date Received by State Agency: _____

Date submitted to Ethics Commission: _____

Governmental agency submitting Disclosure: _____



STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Casepoint, LLC

Authorized Signature: [Signature] Date: 12/19/2019

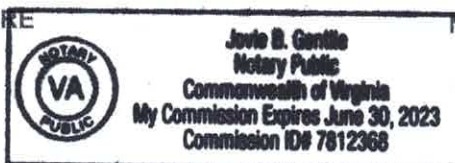
State of Virginia

County of Fairfax, to-wit:

Taken, subscribed, and sworn to before me this 19th day of December, 2019.

My Commission expires June 30th, 2023.

AFFIX SEAL HERE



NOTARY PUBLIC Jovie Gentile [Signature]

Purchasing Affidavit (Revised 01/19/2018)

1. Casepoint Standard Terms and Conditions

1.1. Definitions.

The following terms used in these Standard Terms and Conditions shall have the following meanings:

"Affiliate" means, for either Party, any entity that directly or indirectly controls, is controlled by, or is under common control with that Party, where "control" means the power to direct the management and policies of an entity, whether through majority ownership of voting securities or by contract.

"Authorized User" means any individual who is an employee of Client or such other person or entity as may be authorized by an Order (e.g., a third party providing services to Client), authorized, by virtue of such individual's relationship to, or permissions from, Client, to access the Casepoint Platform pursuant to Client's rights under this Agreement.

"Case" shall mean the litigation described in the Case Initiation Form.

"Case Initiation Form" shall mean the form that initiates a new case or matter for which the Services described in the Order are to be provided.

"Casepoint Platform" means the software developed and owned or licensed by Casepoint and offered to Clients as a service.

"Client Information" means all ESI (Electronically Stored Information) provided to Casepoint from whatever source and all Client instructions.

"eDiscovery" means the process of identifying, locating, preserving, collecting, preparing, reviewing and producing ESI in the context of the legal process.

"Effective Date" means the start date of the contract or the latest signature date of the contract.

"Electronically Stored Information" or "ESI" is used as referenced in the United States Federal Rules of Civil Procedure and means information that is stored electronically, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard/paper copy.

"European Personal Information" means any information received by Casepoint from Client, or on behalf of Client, that is sufficient to cause a natural person who is a citizen of Europe to be identified, directly or indirectly.

"Gigabyte Calculation" means the measurement of the data size, in GBs, of Client Data stored on Casepoint servers.

"Optical Character Recognition (OCR)" means the recognition of text characters by a computer and conversion to searchable text.

"Order" shall mean the combination of the agreement and statement of work signed by both parties.

"Service Limits" means the limitations on the use of a particular Service as set forth on the Order.

"Services" shall mean the access to Casepoint eDiscovery and other services specified in an Order to be provided under the terms of this Agreement.

"Technology Assisted Review (TAR)" means the process for prioritizing or coding a collection of ESI utilizing the Casepoint Platform based upon Client's review of a document subset and judgment of the subject matter.

***Terms not otherwise defined in this Agreement shall have the definitions set forth in *The Sedona Conference Glossary: E-Discovery & Digital Information Management* (Fourth Edition, 2014).

1.2. Access and Use.

- A. Provision of Services.** Subject to the terms and conditions contained in this Agreement, Casepoint agrees to provide the Services ordered by Client as set forth in the Statement of Work below.
- B. Provision of Access.** Subject to the terms and conditions contained in this Agreement, Casepoint hereby grants to Client and its Authorized Users a non-exclusive, non-transferable right to access the features and functions of the applicable Casepoint Platform set forth in the applicable Order during the applicable access term set forth on the Order by the Authorized Users for the given Case and for no other purposes. On or as soon as reasonably practicable after the Effective Date, Casepoint shall provide to Client the necessary passwords, security protocols and policies and network links or connections and access protocols to allow Client and its Authorized Users to access the Casepoint Platform. Client and any Authorized User may only use the Casepoint Platform in accordance with the access protocols. Each Authorized User must be a single named individual and in no event may passwords or user accounts be shared. If an Authorized User is limited to viewing reports then in no event shall such Authorized User attempt to create reports in any manner.
- C. Usage Restrictions.** Client shall not: (i) use the Casepoint Services in excess of the Service Limits; (ii) use the Casepoint Platform or Casepoint Services for any litigation other than the applicable Case; or (iii) allow third parties other than Authorized Users to gain access to the Casepoint Services or Casepoint Platform. Client will ensure that

its use of the Casepoint Service and Casepoint Platform complies with all applicable laws, statutes, regulations or rules.

- D. Authorized Users.** Access to Services and Casepoint Platform. Client may permit any Authorized Users to access and use the features and functions of the Casepoint Platform as contemplated by this Agreement. Client will be responsible for all actions or omissions of its Authorized Users. Authorized User IDs cannot be shared or used by more than one Authorized User at a time. Client shall use commercially reasonable efforts to prevent unauthorized access to, or use of, the Casepoint Platform and shall notify Casepoint promptly of any such unauthorized use known to Client. Client acknowledges and agrees that it may need certain networking capabilities, bandwidth and hardware to use the Casepoint Platforms. Client is solely responsible for all hardware, software, Internet connectivity and bandwidth required to reach the Casepoint systems to gain access to the Casepoint Platforms.
- E. Service Rules and Guidelines.** Client and all Authorized Users shall use the Casepoint Platforms solely for its internal purposes as contemplated by this Agreement and shall not use the Casepoint Platform to: (i) transmit material containing software viruses or other harmful or deleterious computer code, files, scripts, agents, or programs; (ii) interfere with or disrupt the integrity or performance of the Casepoint Platform or the data contained therein; (iii) attempt to gain unauthorized access to the Casepoint Platform, computer systems or networks related to the Casepoint Platform; or (iv) interfere with another user's use and enjoyment of the Casepoint Platform.
- F. Third Party Software.** The Casepoint Platform may provide access to certain third party software and plug-ins (the "Third Party Software"). The Third Party Software, primarily libraries from Microsoft®, and other software vendors are bundled with the Casepoint Platform and are subject to separate license terms that are not covered under this Agreement. Any such separate license terms are provided in a text file accompanying this individual third-party module. The Third Party Software is not part of the Casepoint Platform.

1.3. Payment.

- A. Fees.** In consideration for the access rights granted to Client and the Services performed by Casepoint under this Agreement, Client will pay to Casepoint, without offset or deduction, all fees required as described in this Agreement. All fees will be billed and paid in U.S. dollars.
- B. Payment Terms.** Monthly hosting charges shall be invoiced monthly based upon the Gigabyte Calculation for a given month, payable in net 30 calendar days. Professional services invoices shall be invoiced in accordance with the Order, payable in net 30 calendar days. Payments are to be made in US dollars. If Client has unpaid invoices,

invoiced amounts shall accrue interest at the rate of 1.5% per month from the due date. Casepoint reserves the right to suspend access to the Casepoint software and services with prior notification to Client if payments are 45 or more days past due.

- C. Disputed Fees.** If Client disputes any fees, taxes, or other charges billed by Casepoint, Client shall notify Casepoint, in writing, of the disputed amount and any relevant information regarding the circumstances of the dispute. Casepoint shall acknowledge receipt of the dispute information in writing to Client. All parties agree to work cooperatively to resolve any such disputed amounts. If the Client fails to provide Casepoint with a notice of such a disputed amount within twenty (20) business days following receipt of Casepoint's invoice for such disputed charge, then such amount is deemed undisputed and due to Casepoint.
- D. Taxes.** Client will be responsible for payment of any applicable sales, use and other taxes and all applicable export and import fees, customs duties and similar charges (other than taxes based on Casepoint's income), and any related penalties and interest for the grant of access rights hereunder, or the delivery of related services, if any. If Client is tax exempt, it shall furnish Casepoint with evidence of its tax-exempt status prior to placing an order for the Casepoint Services. Client will make all required payments to Casepoint free and clear of, and without reduction for, any withholding taxes. Any such taxes imposed on payments to Casepoint will be Client's sole responsibility, and Client will, upon Casepoint's request, provide Casepoint with official receipts issued by appropriate taxing authorities, or such other evidence as Casepoint may reasonably request, to establish that such taxes have been paid.

1.4. Confidentiality, Nondisclosure and Data Security.

- A. "Confidential Information"** means any and all information, which is of a confidential, proprietary or trade secret nature that is furnished or disclosed by one party to the other party or learned by the other party under this Agreement, whether oral, written, or electronic. Without limiting the generality of the foregoing, Confidential Information includes (whether or not marked or identified as confidential, proprietary, or trade secret) the terms and conditions of this Agreement, Client Data, written deliverables, reports and materials generated by Client using the Casepoint Platform, financial, accounting, or tax information, pricing information, and any other information that is marked as "Confidential," "Proprietary," "Trade Secret," or in some other manner to indicate it is of confidential, proprietary or trade secret nature.
- B.** Confidential Information will remain the property of the disclosing party. The receiving party agrees: (i) to hold disclosing party's Confidential Information in strict confidence; (ii) to limit disclosure of disclosing party's Confidential Information to the receiving party's own employees, agents or authorized consultants having a need to know the disclosing party's Confidential Information for the purposes of this

Agreement; (iii) not to disclose any of disclosing party's Confidential Information to any third party; (iv) to use disclosing party's Confidential Information solely in accordance with the terms of this Agreement in order to carry out its obligations or exercise its rights under this Agreement; and (v) to notify the disclosing party promptly of any unauthorized use or disclosure of the Confidential Information and to cooperate with the disclosing party in every reasonable way to cease such unauthorized use or disclosure.

- C. The confidentiality obligations under this Section 1.4 will not apply to information that the receiving Party can demonstrate: (i) at the time of disclosure is generally available to the public; (ii) has become generally available to the public through no breach of this Agreement or other wrongful act by the receiving Party; (iii) is independently developed by the receiving Party without regard to the Confidential Information of the other Party; or (iv) is required to be disclosed by law or order of a court of competent jurisdiction or regulatory authority, provided that the receiving Party shall attempt in good faith to furnish prompt written notice of such required disclosure to the disclosing Party and reasonably cooperate with the disclosing Party, at the disclosing Party's expense, in any effort made by the disclosing Party to seek a protective order or other appropriate protection of its Confidential Information.
- D. The parties agree that any breach of the confidentiality obligations set forth herein may cause the disclosing Party substantial and irreparable damages; therefore, if the receiving Party discloses or uses (or threatens to disclose or use) any Confidential Information of the disclosing Party in breach of this Section 1.4, the disclosing Party shall have the right, in addition to any other remedies available to it, to seek injunctive and equitable relief.
- E. Casepoint acknowledges that Client Data includes or may include data that requires special protection, such as personally identifiable information ("PII") of non-parties ("PII" meaning any information that, alone or in combination with other information, relates to an identifiable individual, such as first and last name, Social Security number, telephone number, e-mail address, home address, driver's license number, passwords, and financial account information). Casepoint will store all Client Data in a segregated manner and such Client Data will not be commingled with other Casepoint clients' data. Client shall at all times be responsible for advising Casepoint of any necessary standard physical, technical, administrative, and organizational safeguards to protect Client Data from unauthorized access, use, disclosure, theft, loss or destruction ("Data Breach"). Such measures may include (without limitation) firewalls, encryption, system monitoring and testing, disaster recovery and backup, which Casepoint may agree to implement for additional fees. Absent such agreement, Casepoint shall not be liable in the event of a Data Breach resulting from any cause including (without limitation) as a result of any malicious intrusion, or any act or omission the is a result of intentional or grossly negligent misconduct on the part of

Casepoint, its agents or representatives, except that Casepoint shall (i) immediately notify Client in writing of the Data Breach and furnish Client with details of the breach ascertainable from Casepoint servers.

- F. Upon termination or expiration of this Agreement, Casepoint shall deliver all Client Data to Client or to such other person or entity as directed by Client in a format and by delivery means specified by Client, after all outstanding payments have been made. After Client has notified Casepoint that Client has received its Client Data, Casepoint will comply with any direction from Client to destroy any copies of Client Data remaining in Casepoint's possession, custody, or control. With regard to all materials other than Client Data, Casepoint and Client shall each deliver to the other, or at the election of the Party to whom delivery would otherwise be made, destroy, all documents, data, and other information that were provided in connection with this Agreement, including Confidential Information.
- G. Client and its Authorized Users shall have access to the Client Data and shall be responsible for all changes to and/or deletions of Client Data and the security of all passwords and other access protocols required in order to access the Casepoint Platforms. Casepoint will use industry standard means to protect the Client Data from unauthorized access. Client shall have the ability to export Client Data out of the Casepoint Platforms and is encouraged to make its own back-ups of the Client Data. Client shall have the sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Client Data.

1.5. Client Data.

- A. **Client Data.** "Client Data" means: (i) all data delivered to Casepoint by or on behalf of Client, its Affiliates, in connection with use of the Casepoint Platform by or on behalf of Client; (ii) all data collected, provided, or stored through use of the Casepoint Platform by or on behalf of Client; and (iii) any reports, analyses, summaries, data bases, and any other information and material derived or compiled from Client Data. Notwithstanding the foregoing, Client Data shall not include administrative and system technical data generated by Casepoint or the Casepoint Platform in the course of providing the services, such as, by way of example and not limitation, server log files, hardware error reports, and software bug reports, all of which shall be the property of Casepoint.
- B. **Ownership of Client Data.** Client shall be the sole and exclusive owner of all right, title, and interest in and to the Client Data. Nothing in this Agreement shall be construed in any way as restricting Client's right to full use and enjoyment of Client Data in any manner as determined by Client in its sole discretion including (without limitation) (i) Client's right to create, reproduce, store, and share with any person or entity, texts, reports, lists, or other compilations of Client Data produced, downloaded, or compiled using the Casepoint Platform, and (ii) Client's right to work with an alternative provider

of services to implement a successor data management system in advance of or after expiration or termination of this Agreement for any reason.

- C. Casepoint's use of Client Data.** Client hereby grants to Casepoint a limited, non-exclusive license to use Client Data solely as needed to perform Casepoint's obligations under this Agreement. Casepoint shall not use, sell, rent, transfer, distribute, or otherwise disclose or make available Client Data for Casepoint's own purposes or for the use or benefit of any person or entity other than Client except as directed by Client.
- D. Requests for Client Data.** Casepoint shall deliver to Client or such other person or entity as directed by Client, a complete and fully up-to-date copy (i.e. an extract) of Client Data in a format determined by Casepoint in accordance with the charges set forth on the Order Form. All outstanding and forthcoming invoices must be paid before such extract will be released to Client.
- E. European Personal Information.** Client agrees that it shall inform Casepoint of any required corrections, deletions, blocking and/or making available European Personal Information. Casepoint shall notify Client promptly of any request it receives regarding European Personal Information that is contained, or alleged to be contained, within Client Data. It shall be Client's obligation and duty to investigate the request; to the extent that changes to the data are required, Casepoint will provide commercially reasonable cooperation to facilitate compliance with Client's instructions. Client acknowledges and agrees that some instructions, including destruction or return of data, may result in additional fees.

1.6. Data Handling.

- A. Exception Handling.** All Client Data will be processed using automated technology and exception reports for Client Data that could not be processed will be provided.
- B. File Types.** Casepoint automated processing tools attempts to process only files listed in the approved processing file list found here:
<https://www.casepoint.com/approvedfilelist> and Casepoint shall not be responsible for providing the Services for any other file types.

1.7. Warranties.

- A.** Casepoint represents and warrants that it will provide the Service and perform its other obligations under this Agreement in a professional and workmanlike manner substantially consistent with general industry standards. Casepoint further warrants, for the benefit of Client only, that the Casepoint Platform will conform in all material respects to the standard user documentation for such Casepoint Platform provided to Client by Casepoint (the "Documentation") for a period of thirty (30) days after

Casepoint makes the Casepoint Platform available to Client, provided that such warranty will not apply to failures to conform to the Documentation to the extent such failures arise, in whole or in part, from (i) any use of the Casepoint Platform other than in accordance with the Documentation, or (ii) any combination of the Casepoint Platform with software, hardware or other technology not provided by Casepoint under this Agreement.

- B.** Casepoint warrants that it provides adequate protections in accordance with the requirements of Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016. Casepoint represents that it self-certifies to and complies with EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, as administered by the US Department of Commerce, and shall take reasonable steps to maintain its self-certifications to maintain compliance with the Privacy Shield Framework with respect to Processing European Personal Information when providing services under this Agreement.
- C.** Client and Casepoint each represents and warrants that it, and any individual signing on its behalf, has full authority to (i) execute this Agreement and (ii) bind itself to this Agreement.
- D. DISCLAIMER.** EXCEPT FOR THE WARRANTIES MADE HEREIN, CASEPOINT MAKES NO WARRANTY, EXPRESS OR IMPLIED, REGARDING THE ACCURACY, USEFULNESS OR RESULTS OF ANY RECOMMENDATIONS MADE VIA THE SOFTWARE. THERE IS NO WARRANTY THAT INFORMATION WITHIN THE SOFTWARE, CASEPOINT'S EFFORTS, OR THE SOFTWARE ITSELF WILL FULFILL ANY OF SUBSCRIBER'S PARTICULAR PURPOSES OR NEEDS. EXCEPT FOR THE WARRANTIES MADE HEREIN, THE SOFTWARE IS PROVIDED "AS IS." THE WARRANTIES PROVIDED UNDER THIS SECTION ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY AND ALL IMPLIED WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE.

1.8. Indemnification.

- A.** Casepoint agrees to indemnify, defend and hold harmless Client and its Affiliates from and against any and all losses, liabilities, costs (including reasonable attorneys' fees) or damages awarded to a third party resulting from any claim by that third party that the Casepoint Platform infringes such third party's patents issued as of the Effective Date, or infringes or misappropriates, as applicable, such third party's copyrights or trade secret rights, provided that Client promptly notifies Casepoint in writing of the claim, cooperates with Casepoint, and allows Casepoint sole authority to control the defense and settlement of such claim. If such a claim is made or appears possible, Client agrees to permit Casepoint, at Casepoint's sole discretion, to enable it to continue to use the

Casepoint Platform or to modify or replace any such infringing material to make it non-infringing. If Casepoint determines that none of these alternatives is reasonably available, Client shall, upon written request from Casepoint, cease use of and, if applicable, return such materials that are the subject of the infringement claim. This Section shall not apply if the alleged infringement arises, in whole or in part, from (i) modification of the Casepoint Platform by any party (including, without limitation, Client) other than Casepoint or (ii) combination, operation or use of the Casepoint Platform with other software, hardware or technology not provided by Casepoint, or (iii) related to the Client Data.

- B. Client will indemnify, defend and hold Casepoint and its subsidiaries and Affiliates, harmless against any third-party claim, demand, or action, and any resulting liability, loss, fine, penalty, cost or expense (including, without limitation, reasonable attorney's fees) to the extent arising from or relating to: (i) any allegation that any Client Data infringes any copyright, trademark, trade secret, or any other proprietary right of a third party, or (ii) any Data Breach caused by Client's negligence, (iii) any allegation that Client Data has violated any laws or regulations; or (iv) failure to comply with lawful requests regarding European Personal Information provided that Casepoint promptly notifies Client in writing of the claim, cooperates with Client, and allows Client sole authority to control the defense and settlement of such claim.

1.9. Limitation of Liability.

- A. Client acknowledges that it alone is responsible for the results obtained from its use of the Casepoint Platform and Services, including without limitation the completeness, accuracy and content of such results.
- B. IN NO EVENT SHALL CASEPOINT BE LIABLE FOR INCIDENTAL, INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, REGARDLESS OF THE NATURE OF THE CLAIM, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, COSTS OF DELAY, FAILURE OF DELIVERY, BUSINESS INTERRUPTION, OR LIABILITIES TO THIRD PARTIES ARISING FROM ANY SOURCE (EVEN IF THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES). THIS LIMITATION UPON DAMAGES AND CLAIMS IS INTENDED TO APPLY WITHOUT REGARD TO WHETHER OTHER PROVISIONS OF THIS AGREEMENT HAVE BEEN BREACHED OR HAVE PROVEN INEFFECTIVE. CASEPOINT'S ENTIRE LIABILITY AND CLIENT'S EXCLUSIVE REMEDY FOR DAMAGES FOR ANY CLAIMS ARISING UNDER OR IN CONNECTION WITH THIS AGREEMENT, REGARDLESS OF THE CAUSE OF ACTION, WHETHER IN CONTRACT OR IN TORT (INCLUDING WITHOUT LIMITATION, BREACH OF WARRANTY AND NEGLIGENCE CLAIMS), SHALL BE LIMITED TO THE AMOUNT PAID FOR THE CLIENT APPLICATION AND SERVICES IN THE TWO MONTH PERIOD PRIOR TO THE EVENT GIVING RISE TO THE CLAIM. THE EXISTENCE OF MULTIPLE CLAIMS WILL NOT SERVE TO ENLARGE THIS LIMITATION. TO THE EXTENT THAT ANY JURISDICTION PRECLUDES THE LIMITATION OF

CONSEQUENTIAL OR SPECIAL DAMAGES, THE PARTIES NONETHELESS AGREE THAT THE SCOPE, DURATION AND EXTENT OF DAMAGES SHALL BE THE MINIMUM PERMITTED BY LAW. THE WARRANTY DISCLAIMER AND LIMITATIONS OF LIABILITY ARE FUNDAMENTAL ELEMENTS OF THE BASIS OF THE BARGAIN BETWEEN Client AND Casepoint. Casepoint WOULD NOT PROVIDE THE CASEPOINT PLATFORM OR SERVICES TO Client IN THE ABSENCE OF SUCH DISCLAIMER AND LIMITATIONS.

1.10. Publicity.

Upon execution of this Agreement by the Parties, Casepoint may publish Client's name and company logo on Casepoint's website and other marketing material.

1.11. Term and Termination.

- A. Term.** The term of this Agreement will commence on the Effective Date and will continue for a period of the latter to occur of (i) one (1) year thereafter and (ii) the last effective access term as set forth in an Order (e.g., the period of performance of a Statement of Work), unless earlier terminated in accordance with this Section. This Agreement will automatically renew for successive one (1) year terms unless either Party provides written notice of its desire not to renew at least thirty (30) days prior to the expiration of the then-current term (the initial term, together with any renewal terms, collectively, the "Term").
- B. Termination for Breach.** Either Party may, at its option, terminate this Agreement in the event of a material breach by the other Party. Such termination may be affected only through a written notice to the breaching Party, specifically identifying the breach or breaches on which such notice of termination is based. The breaching Party will have a right to cure such breach or breaches within thirty (30) days of receipt of such notice, and this Agreement will terminate in the event that such cure is not made within such thirty (30)-day period.
- C. Termination Upon Bankruptcy or Insolvency.** Either Party may, at its option, terminate this Agreement immediately upon written notice to the other Party, in the event (i) that the other Party becomes insolvent or unable to pay its debts when due; (ii) the other Party files a petition in bankruptcy, reorganization or similar proceeding, or, if filed against, such petition is not removed within ninety (90) days after such filing; (iii) the other Party discontinues its business; or (iv) a receiver is appointed or there is an assignment for the benefit of such other Party's creditors.
- D. Effect of Termination.** Upon any termination of this Agreement, Client will (i) immediately discontinue all use of the Casepoint Platform and any Casepoint Confidential Information; and (iii) promptly pay to Casepoint all amounts due and payable under this Agreement.

- E. Survival.** The provisions of Sections 1.4, 1.5, 1.7(D), 1.8(B), 1.9(B), 1.10, 1.11(D), 1.11(E), and 1.12 will survive the termination of this Agreement.

1.12. Governing Law and Disputes.

- A. Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia without regard to its conflicts of laws rules, except that the Virginia Uniform Computer Information Transaction Act shall not apply to this Agreement.
- B. Dispute Resolution.** Notwithstanding any Federal or State law to the contrary, in the event of a dispute arising out of this agreement, the Parties may agree to submit the dispute to arbitration, which if so agreed shall be arbitrated in Virginia by a recognized, established, alternative dispute resolution (ADR) firm agreed to by the parties. The arbitration shall be conducted in accordance with the discovery rules of the Federal Rules of Civil Procedure and in accordance with the Federal Rules of Evidence, unless modified by agreement of the parties. In the event the Parties are unable to mutually agree to arbitration, or upon mutually agreeing to arbitration are unable to agree upon an ADR firm to arbitrate the parties dispute, the Parties agree that the courts of Fairfax County, Virginia shall have exclusive jurisdiction over such disputes and they shall be presented to the (same) and be resolved in accordance with the applicable Rules of these courts. The parties agree that the claim period for a dispute is one year from the disputed action.

1.13. General.

- A.** Any notice or other communication required or permitted to be made or given by either Party pursuant to this Agreement must be in writing, in English, and will be deemed to have been duly given: (i) five business days after the date of mailing if sent by registered or certified U.S. mail, postage prepaid, with return receipt requested; or (ii) one business day after being sent by express courier service or by email when combined with a “delivered” and “read” receipt. All notices must be sent to the other Party at its address as set forth on the first page or at such other address as such party will have specified in a notice given in accordance with this Section.
- B.** This Agreement will be binding upon and inure to the benefit of the Parties, their successors and permitted assigns.
- C.** The section headings contained herein are for reference only and shall not be considered substantive parts of this Agreement.
- D.** United States Government End Users – This Casepoint Platform and the software and documentation associated with it are developed exclusively with private funds and constitute a “commercial item” as defined at 48 C.F.R. 2.101, consisting of

“commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 227-7202-1 through 227-7202-4 and their related counterparts in the DFAR. This Casepoint Platform is licensed only as commercial computer software and commercial computer software documentation and only with the rights granted to public users generally as set forth in this Agreement. If any portion of the software is deemed “noncommercial,” or the following FARs or DFARs are deemed to apply, the software is licensed under the terms hereof and under RESTRICTED RIGHTS set forth in 48 C.F.R. 52-227-14, 48 C.F.R. 252-227-7013 and -7014, FAR 52.227-19 Commercial Computer Software—Restricted Rights and DFAR 252.227-7013 Rights in Technical Data and Computer Software.

- E. If any provision of this Agreement is invalid or unenforceable for any reason in any jurisdiction, such provision will be construed to have been adjusted to the minimum extent necessary to cure such invalidity or unenforceability. The invalidity or unenforceability of one or more of the provisions contained in this Agreement will not have the effect of rendering any such provision invalid or unenforceable in any other case, circumstance or jurisdiction, or of rendering any other provisions of this Agreement invalid or unenforceable whatsoever.
- F. No failure or delay by either party in exercising any right, power or remedy will operate as a waiver of such right, power or remedy, and no waiver will be effective unless it is in writing and signed by the waiving party. If either Party waives any right, power or remedy, such waiver will not waive any successive or other right, power or remedy the party may have under this Agreement.
- G. In making and performing this Agreement, Client and Casepoint act and will act at all times as independent contractors, and, except as expressly set forth herein, nothing contained in this Agreement will be construed or implied to create an agency, partnership or employer and employee relationship between them. Except as expressly set forth herein, at no time will either Party make commitments or incur any charges or expenses for, or in the name of the other Party.
- H. This Agreement sets forth the entire agreement and understanding between the Parties with respect to the subject matter of this Agreement and, supersedes and merges all prior oral and written agreements, discussions and understandings between the Parties with respect to the subject matter of this Agreement, and neither of the Parties will be bound by any conditions, inducements or representations other than as expressly provided for in this Agreement.
- I. The Parties acknowledge that the covenants set forth in this Agreement are intended solely for the benefit of the Parties, their successors and permitted assigns. Nothing herein, whether express or implied, will confer upon any person or entity, other than the Parties, their successors and permitted assigns, any legal or equitable right whatsoever to enforce any provision of this Agreement.

- J. Casepoint shall not incur any liability for failure to perform any of its obligations under this Agreement in the event of a Force Majeure Event. A “Force Majeure Event” means an event beyond the reasonable control of Casepoint including, without limitation, an act of God, war, riot, civil commotion, malicious damage, compliance with a law or governmental order, rule, regulation or direction, accident, fire, flood and storm, and/or technical or service interruption not due to the negligence of Casepoint.

[END OF CASEPOINT STANDARD TERMS AND CONDITIONS.]

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ ISC2000000011

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

<input type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

C ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ C

Company

Amy Hilbert

Authorized Signature

12 ☐ 2020

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.
Revised 6/8/2012