



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 # 1

[List View](#)

General Information Contact Default Values Discard Document Information Contribution Request

Procurement Folder: 1616078

Procurement Type: Central Contract - Fixed Fee

Vendor ID: US000840388

Legal Name: SURGE-AVALON HOLDINGS INC

Alias/DBA:

Total Bid: 333,790.00

Response Date: 8/16/2025

Response Time: 12:28

Responded By User ID: elapane

First Name: Emily

Last Name: Lapane

Email: emily.lapane@seckman.co

Phone: 7573258911

SO Doc Code: CRPD

SO Dept: 0034

SO Doc ID: 00725000000417

Published Date: 3/3/25

Close Date: 3/7/25

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum No 2 Cybersecurity e-Discovery SAAS (DT251Q)

Total of Header Attachments: 1

Total of All Attachments: 1



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

State of West Virginia
Solicitation Response

Proc Folder: 1619676		
Solicitation Description: Addendum No 2 Cybersecurity e-Discovery SAAS (OT25112)		
Proc Type: Central Contract - Fixed Amt		
Solicitation Closes	Solicitation Response	Version
2025-03-07 13:30	SR 0231 ESR03062500000005363	1

VENDOR

VS0000048200
SURGE AVALON HOLDINGS INC

Solicitation Number: CRFQ 0231 OOT2500000017

Total Bid: 33700

Response Date: 2025-03-06

Response Time: 12:20:17

Comments:

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor
Signature X

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				33700.00

Comm Code	Manufacturer	Specification	Model #
43231511			

Commodity Line Comments: Exhibit A Pricing Page attached to uploaded proposal documents.

Extended Description:

Please see the attached Exhibit A Pricing Page
Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.



EDISCOVERY SERVICES

WEST VIRGINIA OFFICE OF TECHNOLOGY

3.4.25



Emily LaPane
Regional Account Executive
eDiscovery Southeast
Surge Avalon Holdings Inc
emily.lapane@teamavalon.com

5650 Breckenridge Parkway, Suite 103
Tampa, FL 33610
www.teamavalon.com

Dear Mr. Welch,

Thank you for considering Avalon for your secure eDiscovery needs. We know this is an important part of your business process and are honored to have the opportunity to provide such critical services.

At Avalon, our mission is: "Save the day, every day." To us, that means we're always looking for new ways to help our clients succeed by handling projects that are too large, complex, and time-sensitive to handle in-house – like your eDiscovery needs – and to add value every step of the way.

We are particularly well-positioned to provide eDiscovery services to the West Virginia Office of Technology because of our structure, culture, and suite of services, and feel you will be hard-pressed to find another company that can deliver the customer experience and innovative solutions you expect.

Here's why:

- Our litigation support team **works with 850+ law firms annually**, more than 40 of which are Am Law 100 firms.
- Avalon currently **hosts hundreds of cases every month**, ranging in size from hundreds of gigabytes to multiple terabytes.
- We develop **custom standard operating procedures (SOPs)** designed to integrate quality control at every step of the process.
- Avalon will provide your firm with **strategic, customized solutions**. Unlike some of the other eDiscovery providers in the marketplace, we do not employ a one size fits all model.
- We are a **SOC 2 Type 1 vendor**, and our **cybersecurity division** provides both proactive and reactive security services to organizations across the country. You will not find another litigation support company that understands security and confidentiality as thoroughly as we do.
- Our Net Promoter Score (NPS) is 92. We are very proud of this rating, as we are **passionate about customer service**, and this score proves that our clients are highly satisfied with the products and services our team provides. We have a culture of being creative and nimble, and a team who will do whatever it takes to **get the job done, day in and day out**.

We look forward to the opportunity to present this proposal to you, so we may explain in detail exactly why Avalon would be the ideal partner to tackle your eDiscovery challenges.

Sincerely,

Emily LaPane

Every company – and every job – is different, so you need a managed eDiscovery partner that can develop strategic processes and workflows and provide access to the most powerful technology in the industry. Avalon's hyper-responsive team members are experts in the field; knowledgeable, dedicated to your needs and goals, and capable of using our superior technology and tried-and-true processes to get the job done.



MISSION

SAVE THE DAY, EVERY DAY.

COMPANY CERTIFICATIONS & AWARDS

- SOC 2 Type 1 Certified Vendor
- RelativityOne Silver Partner
- 90+ Net Promoter Score (NPS)

APPLE = 72

STARBUCKS = 77

RITZ CARLTON = 78

AVALON = 90+ ★

When you partner with Avalon, you can expect:

WE ARE LITIGATION SUPPORT SPECIALISTS

Achieve more at your firm by taking advantage of Avalon's highly specialized litigation support services, including eDiscovery, managed review, digital forensics, cybersecurity, managed office services, paper discovery, legal staffing, and appellate services. Our hyper-responsive project and account managers, technicians, and solutions architects will cultivate a close relationship with your team to determine how we can best fulfill your firm's needs, then provide unwavering support throughout our partnership. You can rest assured, knowing we take privacy and security seriously, as we're a SOC 2 Type 1 compliant service provider, and our designation as a RelativityOne Silver Partner means you can expect the highest caliber of customer service.

EDISCOVERY

Every case is different, so you need an eDiscovery partner that can develop strategic processes and workflows and provide access to the most powerful technology in the industry. Avalon's team members are experts in the field; knowledgeable, dedicated to your needs and goals, and capable of using that superior technology and those tried-and-true processes to reveal the data you need. We are a SOC 2 Type 1 compliant service provider and, as a RelativityOne Silver Partner, we are known for delivering innovative ways of thinking as well as providing exceptional service to our clients.

MANAGED EDISCOVERY

Legal teams are often frustrated by the inability to budget accurately when it comes to the inconsistent cost of eDiscovery, whether their support is internal or outsourced. The continued investments in the latest technology, training of staff, and expensive infrastructure are at odds with the desire for dedicated services at a predictable cost.

To help combat these challenges for our clients, Avalon offers a managed eDiscovery services program. Our comprehensive eDiscovery services are available in a subscription-based package, which eliminates the unpredictable cost aspect of electronic discovery. In addition, we are dedicated to implementing the newest, most innovative eDiscovery solutions, so you'll always have state-of-the-art technology at your fingertips.

STATE-OF-THE-ART EQUIPMENT & TECHNOLOGY

Partner with Avalon for your next case and take advantage of some of the most powerful eDiscovery tools in the world. As a RelativityOne Silver Partner, Avalon is known for delivering innovative solutions, as well as an exceptional service experience, to our eDiscovery clients. Rest assured, we will provide and be responsible for all equipment and technology needed to complete your forensics, eDiscovery, and managed review projects.

THE HIGHEST LEVEL OF SECURITY & CONFIDENTIALITY

Security is paramount to everything we do at Avalon and that is no different for our managed eDiscovery services. We have several protocols in place to ensure your confidential data is handled with the utmost respect for your – and your clients’ – privacy. We are a SOC 2 Type 1 compliant service provider, and have an entire division devoted to cybersecurity.

CERTIFIED TO ASSIST YOU

In addition to years of industry experience, Avalon’s consultants hold certifications including: Cellebrite’s CCO and CCPA for mobile device forensics, McAfee CCII and CPCI for cybersecurity and criminal investigations, and COSFE from PassMark for digital investigation tools. They are also available to provide expert testimony, if needed.

A DEDICATED CASE TEAM

From forensic collections and analysis to data hosting and review, your dedicated project manager will lead your highly experienced team throughout the project, so that no time will be wasted bringing team members up to speed. We also understand that your needs may fluctuate, so your case team can be scaled up or down as required to keep your budget and resources in line.

WE OFFER C-SUITE ACCESSIBILITY

At Avalon, the “C” in “C-suite” stands for “Committed to our Clients.” While you have access to all our subject matter experts, we also realize that sometimes you need to speak to a C-level executive directly. Each member of the leadership team is available to personally answer your questions or provide insight into your challenges – and is 100% happy to do it.

WE GUARANTEE THE HIGHEST LEVEL OF QUALITY CONTROL

Every service provided through Avalon shares one common element: the details matter. Putting quality first is a mindset ingrained in everything we do. As a result, we have several quality control processes and procedures in place to ensure the highest quality work, and each of our team members is trained specifically to find and eliminate errors. We go above and beyond to make sure your project is accurate, so you don’t have to think twice about it.

The West Virginia Office of Technology has a unique set of needs, capabilities, and expertise, so the Avalon team will work with you to build an offering based on your current and future requirements. Perhaps that means we provide you with access to robust processing tools to enhance your internally managed document review platforms. Or maybe you rely on us for both processing and hosting solutions. Whatever option you choose, Avalon's managed eDiscovery services program delivers exactly what your firm requires to handle the most complex electronic discovery challenges for your clients.

LITIGATION SUPPORT

If your firm already has its own infrastructure, our litigation support professionals, who have experience with multiple platforms, can serve as an extension of your team.

SOFTWARE AS A SERVICE (SAAS)

We provide the software and infrastructure support, while your staff handles the work.

ALL-INCLUSIVE

Avalon offers full case management from start to finish, handling all aspects of eDiscovery: ingestion, processing, hosting, and production; your staff only has to review document.

HYBRID

Take advantage of Avalon's expertise and experience when needed, but manage your costs by handling some of the work in-house; blocks of hours may be purchased.

MASTER SERVICES AGREEMENT (MSA)

By agreeing to use Avalon exclusively for specific services, your firm receives predictable pricing and experienced support.

BENEFITS OF MANAGED EDISCOVERY SERVICES:

- Cost predictability
- Scalability of case teams, as required
- Process standardization
- No technology obsolescence
- No technology investment
- Cost recovery
- Limited investment in project managers and/or technology managers

MANAGED EDISCOVERY SERVICE ADD-ONS:

- Cybersecurity services
- Collections
- Data processing
- Managed review, contract analysis
- Relativity legal hold
- Near-line/cold storage
- Monthly bundled tech & project management time

Over the last several years, many industries have shifted toward cloud solutions for the benefits of scale and performance, improved security, and rapid innovation. The unique capabilities of the cloud enable Relativity – and Avalon – to deliver a game-changing experience in RelativityOne to the team at the West Virginia Office of Technology.

Here are a few of the key benefits RelativityOne provides:



Security – RelativityOne is built on a secure foundation with Microsoft Azure which has over 3,500 dedicated cybersecurity experts, secure network infrastructure, and robust testing and monitoring. On-premises technology has limitations that do not enable the same proactive approach to security.



Performance – RelativityOne can be leveraged on projects of any size – from small internal investigations to the largest, most complex matters in the world. Its sophisticated backend technology enables median document load times of 0.22 seconds. Server customers may experience up to ten times slower document load times.



Feature set & product experience – Cloud technology allows RelativityOne to iterate faster and deliver certain functionality that can't be replicated for an on-premises solution. Examples include Collect in RelativityOne for remote data collections, Redact in RelativityOne to automate redactions, and activity and utilization dashboards that help you maximize your subscription and protect your data.



Workflow automation – Cloud-enabled automation across the platform – including case set up and analytics with Automated Workflows, and integrated automated redaction capabilities with Redact in RelativityOne – allows you to save time, while reducing human error. Due to limitations in Server, the same automation capabilities can't be built in.



Scalability – Since RelativityOne is cloud-based, you have access to a range of computing resources, so you can scale up or down depending on your case requirements. Using on-premises software means your processes are limited by the available hardware, which limits your ability to handle complex cases and large amounts of data.

As a RelativityOne Silver Partner, Avalon stands out against our competition for not only providing our eDiscovery clients with best-in-breed technology, but also by delivering the highest level of service to ensure complete customer satisfaction. The RelativityOne Silver Level is part of the Relativity Partner Program and recognizes organizations that have reached a high bar for experience, customer satisfaction, and staff training and certifications. Avalon is proud to be one of just 16 RelativityOne Silver Partners in the world, and hope to share our expertise and RelativityOne's superior technology with the team at the West Virginia Office of Technology.



EMILY LAPANE

Regional Account Executive eDiscovery Southeast

WORK EXPERIENCE

Avalon

Regional Account Executive eDiscovery Southeast
July 2024 - Present

An Account Executive is responsible for meeting sales and revenue goals by selling services to new and existing clients in designated markets

- Build and maintain a network of sources from which to identify new sales leads.
- Generate sales by meeting with prospective and existing clients.
- Communicate with clients and gather information about project's scope, budget, and timelines.
- Manage the entire sales cycle from inception to delivery.
- Prepare SOWs (Statements of Work).
- Meet/exceed yearly quota set with Managing Partner.
- Coordinate meetings with aging buyers for assigned territory.
- Manage brokered vendors on work that can't be performed in house.
- Write up jobs based on the scope of the project.
- Work closely with Operations team to ensure project deadlines are being met.
- Communicate all large project deadlines with department leaders.
- Invoice completed jobs and delivery to clients as needed.
- Attend and participate in Review and Planning sales meetings.
- Maintain and track sales activity through CRM tool.



EMILY LAPANE

Regional Account
Executive eDiscovery
Southeast

CARET Legal **Enterprise Sales Development Representative** **August 2023 - July 2024**

- Team of five BDRs + Director of BD consolidated down to myself, alone, as the sole OB source for eight AEs across SMB/MM/Enterprise spaces.
- Have been >210% to quota since hire, including RAMP.
- 460% to quota + 5 closed deals for May '24. PDFs upon request.
- Final month of promotion path into AE role.

Cooper's Hawk Winery **National Wine Club Facilitator/Sales Manager** **October 2018 - March 2021**

- Studied wine under our Master Sommelier, Emily Wines, in Chicago for two years. Coached and developed staff of 45+ locations in sales.
- Responsible for: sales forecasting, metrics, KPIs, customer relationship management, strategic planning/implementation to achieve both long-term success and hyper-growth.

Yelp **Sales and Marketing Manager** **February 2015 - January 2018**

- Core member responsible for Yelp's bicoastal transition from West to East. Created large scale community management hubs, led full-cycle sales for our AdTech SaaS platform, and managed a large-scale team of Community Managers & Brand Ambassadors nationally.
- Negotiated large-scale in-kind trading negotiations on behalf of Yelp with CXO personas across Fortune 100-branded events.
- Networking, strategic relationship building, marketing development (branding, content, SEO, Guerrilla, etc.), sales training, etc.

Wells Fargo **Branch Manager/IFS Dial Team Leader** **February 2012 - June 2015**

- Promoted seven times over a three year span. Top 5 National Seller for Wells Fargo out of thousands - Achieved Platinum Kicker (maxed ICP across five metrics) each month since hire regardless of role, recipient of "Annual STAR Performer", voted "Key to Conversion", Small Business Champion, Matricular Consulate Lead for SPA-speaking prospects.
- Coached, managed and developed a large team of sellers within branch along with leading >200 employees in the IFS phone bank

**EMILY LAPANE**

Regional Account
Executive eDiscovery
Southeast

targeting the 20-50K sector.

- KPI management, consultative selling, CRM, prospecting/lead generation, cold calling, closing deals.

CONTACT**757.325.0911****emily.lapane@teamavalon.com**



PROFILE

Martin has nearly thirty years of experience in the legal field, starting as an attorney before opening his own managed review business. In that time, Martin has received multiple certifications and had his hand in every part of the business, from sales to solutions.



MARTIN MAYNE

Vice President of Growth, Legal Tech

WORK EXPERIENCE

Avalon

VP of Growth, Legal Tech, February 2025 – Present
Solutions Architect, September 2023 – January 2025

Responsible for sustaining and growing revenue across the company in forensic collections, processing, hosting, project management, and applied technologies • Support regional sales team in putting together advanced eDiscovery solutions

Sabbatical/Market Research

January 2022 – August 2023

Occidental Petroleum

eDiscovery Manager, March 2020 – December 2021

Manage all eDiscovery matters from legacy Anadarko and Oxy litigation docket as well as internal investigations • Collections/processing/hosting in Recommind's Axcelerate across all data sources • Training for legal departments in case law, eDiscovery issues, best practices, and "deep dive" training • Manage onboarding and training of hundreds of remote platform users

EPIQ (formerly DTI)

Solutions Architect, Summer 2018 – March 2020

Supported regional sales team in putting together advanced eDiscovery solutions, combining proprietary and third-party technology, for complex litigation needs • Work closely with collections, processing, hosting, TAR, consulting, information governance, class action, and data breach teams • Certified in demonstrating multiple TAR platforms including NexLP, Brainspace, Blackout, Relativity Active Learning, and Epiq Discovery • Point person for the solutions architect team to develop training and update team on new proprietary processing and review platform, Epiq Discovery • Key player in certifying competence around managed review and TAR tools for management and sales organization

Sales – Legal Solutions, March 2016 – Summer 2018

Promoted to global sales support role focusing on driving growth within document review services • **Result:** Exceeded goal of \$32 million by focusing team on closing client opportunities • Achieved President's Club

**MARTIN MAYNE**

Vice President of
Growth, Legal Tech

**MEMBERSHIPS,
ACTIVITIES
& SPEAKING
ENGAGEMENTS**

Licensed, State Bar of Texas
since 1994; Sedona Working
Group 1; EDRM; Relativity
RCT, RCSP; Brainspace Sales
Certification

eDiscovery conference panels:

ACEDS, Today's General
Counsel, Texas General
Counsel Forum, Carmel Valley
eDiscovery Retreat

**LEARN MORE &
FOLLOW**

teamavalon.com

[Martin on LinkedIn](#)

[Avalon on LinkedIn](#)

Operations/M&A – Document Review Services, June 2012 – March 2016

Key member of the document review services leadership team with a focus on restructuring the business unit, consolidating locations, and integrating personnel to propel growth domestically and internationally

Client Services – Document Review, May 2008 – June 2012

Hired to develop and lead the managed document review platform • Result: Drafted processes and procedures that helped transform the document review platform into a managed service and contractual business supporting 700 review seats in four review centers across the U.S., supported by ten review managers, driving higher overall revenue and profitability for the business

Norton Rose Fulbright

**Discovery Counsel, Information Management Specialist,
February 2005 – May 2008**

Assisted and supervised teams of attorneys in litigation and multinational investigations • Created eDiscovery training for litigation attorney teams and practice support group

Discovery Counsel

Information Management Specialist, August 2004 – January 2005

Managed teams of attorneys and paralegals in document reviews in a variety of databases in matters including patent infringement, patent defense, and white-collar criminal defense cases

Fleming & Associates

Attorney, Supervisor/Project Manager, September 2001 – December 2004

Supervised attorneys and litigation support personnel in massive toxic tort document review and liaised with contractors across the nation for outsourced scanning and objective coding

Private Practice

Criminal Defense Trial Lawyer, May 1994 – September 2001

First and second-chaired trials in federal district court, state district and county courts • Researched, briefed, and argued appeals in federal Fifth Circuit and Texas appellate courts

EDUCATION

University of Houston Law Center Juris Doctorate, 1994

Rice University BA, Managerial Studies, 1988

King's College, University of London Engineering & Philosophy, 1985 – 1986

Rice University Electrical Engineering, 1983 – 1985

CONTACT

212.215.4810

martin.mayne@teamavalon.com



MICHAEL WARREN

Project Manager

WORK EXPERIENCE

**Avalon | Remote
Project Manager
November 2021 – Present**

- Responsible for managing numerous eDiscovery projects from opening to final closeout
- Communicated with clients to acquire project details, advise of expected timelines, discuss phases of work, and proactively address potential concerns
- Actively monitored project status and deadlines, acquired information to minimize project interruptions, and appraised clients of issues or questions as they arose
- Addressed client questions regarding review workflow, use of Relativity, and best practices
- Worked with forensics and technical teams to provide clients with clear and accurate information regarding collections, forensic analysis, exports, processing, and productions
- Daily use of the RelativityOne platform, Microsoft Office, and project management software

**Ryley, Carlock & Applewhite | Grand Rapids, Michigan
Project Lead
September 2017 – November 2021**

- Responsible for managing review, quality control, and production requests for numerous simultaneous e-Discovery projects for major



MICHAEL WARREN

Project Manager

Bar Admission

State Bar of Michigan

-Admitted 2013-

LEARN MORE & FOLLOW

teamavalon.com

[Michael on LinkedIn](#)

[Avalon on LinkedIn](#)

financial litigation

- Coordinated project deadlines and team workflow with other leads, outside counsel, and clients
- Addressed counsel inquiries and requests for assistance
- Worked on short deadlines with attention to detail in matters of responsiveness, redactions, privilege concerns, and particular case-related issues
- Regularly worked overtime and weekend hours in order to meet deadlines and quality standards
- Daily use of Relativity eDiscovery platform, Microsoft Office, and internet research

Document Review Attorney March 2014 – September 2017

- Analyzed documents for relevant to a variety of elements, including responsiveness, privilege, and issue tagging, as well as redacting confidential and privileged information
- Involved in detailed financial, automotive, retail, and environmental document review projects

EDUCATION

Thomas M. Cooley Law School

LL.M. Insurance Law - September 2014
Juris Doctor Cum Laude - January 2012

Calvin College

Bachelor of Arts in History - May 2007

CONTACT

734.846.4264

michael.warren@teamavalon.com

CERTIFICATIONS

Cellebrite's CCO and CCPA
for mobile device forensics

McAfee CCII and CPCI for
cybersecurity and criminal
investigations

COSFE from PassMark for
digital investigation tools



JONATHAN EDWARDS

Senior Forensic Investigator

WORK EXPERIENCE

Avalon
Senior Forensic Investigator
January 2022 – Present

Senior Forensic Investigator for Digital Forensics with a diverse skill set encompassing a wide range of digital forensic incident response (DFIR) specialties, including:

- RAID recovery
- Mobile device examinations
- MacOS and Windows analysis
- Email analysis
- Data recovery
- Deleted data analysis

Kerr County Sheriff's Office
Deputy Sheriff
2014 – 2022

As a Deputy Sheriff, I began working in Corrections and moved to Patrol and was quickly promoted to Corporal and a Field Training Officer. I was awarded commendations for narcotics interdiction and street level investigations.

In 2017, I was promoted to Criminal Investigator at a Sergeant level. This position entailed the daily writing of search warrants, subpoenas, preservation orders, affidavits, and other court orders. While in CID, I began doing digital forensics work as an apprentice in 2019. This digital forensic workflow and forensic environment was an easy transition for me as I had similar working experience doing digital intelligence in the US Navy. I was special commissioned as a Special Deputy US Marshal assigned to the USSS to assist with field partner reporting and digital forensic support for law enforcement.



**JONATHAN
EDWARDS**

Senior Forensic
Investigator

I attended NCFI (National Computer Forensic Institute) in Alabama, hosted by the USSS for MDE and DEI qualifications and training. I attained a CCO (Certified Cellebrite Operator) license through MDE in 2022.

I have 4 years working experience with SQL databases and decoding with Cellebrite and other platforms. I have multiple other trainings and qualifications that are not related but include homicide, child sexual abuse, child physical abuse, child death/ homicide, kidnapping, sex crimes, property crimes, forensic accounting of financials, and others. I have extensive training and experience with advanced Criminal Psychological Interviewing using industry best practices and standards to solicit confessions.

**US Navy
Operations Specialist Petty Officer Second Class (Surface Warfare)
2003 – 2011**

USS Bulkeley (DDG-84), Norfolk, VA | 2003-2004

Assigned as an Operational Specialist involving the gathering, processing, displaying, and evaluating mass amount of data into operational intelligence and actionable intelligence.

USS Gary (FFG-51), Yokosuka, Japan | 2004-2006

Continuing my journey, I was stationed aboard the USS Gary (FFG-51) in Assigned to 7th Fleet as Quick Reaction Force against threats to the US and its allies in the Asia/ Pacific region. Special Warfare selection and team placement 2005- Non-Compliant/ Visit Board Search and Seizure. Security Team Leader for 3 teams of 6 special warfare operators specializing in "shock and awe" tactics of counter-piracy, antiterrorism, and maritime interdiction of human smuggling and narcotics internationally.

USS McCampbell (DDG-85), Yokosuka, Japan | 2006-2008

Special Warfare team reassignment as senior instructor for Close Quarter Combat, Dynamic and Static Room Entry, IFF (Identify Friend or Foe).

***Fleet Air Reconnaissance Squadron 3 (FAIRECRON THREE Det
"Travis"), Northern California | 2008-2011***

Northern California. Most of what I have done with this position was classified and I can say that I was working under a Top-Secret Clearance with PRP (Personnel Reliability Program) assigned under Nuclear Arsenal Readiness. I also was heavily involved in Counterintelligence namely- HUMINT interdiction and ELINT.

**JONATHAN
EDWARDS**

Senior Forensic
Investigator

**LEARN MORE &
FOLLOW**

avaloncyber.com

teamavalon.com

TESTIMONY HISTORY**Criminal investigator/expert witness:**

- 198th and 216th Judicial Districts of Texas

Civil:

- Adecco v Staffworks (6:20-cv-744 MAD/TWD) Northern District of New York, Syracuse Division

CONTACT

716.493.2057

jonathan.edwards@teamavalon.com



JASON HAAG

Operations Support Specialist

WORK EXPERIENCE

Avalon | Remote
Operations Support Specialist
2005 – Present

Jason joined Avalon's imaging department in 2005, there he helped streamline the scanning processes and expand the export formats offered. He was also instrumental in the start and growth of Avalon's eDiscovery department, becoming its first official team member. When Avalon decided to offer Relativity, Jason was responsible for the design, implementation, and maintenance of the Relativity Server instance, while also supporting the IT needs of the eDiscovery and Forensics departments.

With the switch to Relativity One, Jason transitioned into a Project Manager role, where he worked with clients to assist with all areas of the EDRM. He currently is the Operations Support Specialist, where he helps develop and maintain the processes, procedures, and applications used by the eDiscovery team.

CONTACT

315-471-3333

jason@teamavalon.com

LEARN MORE &

PROFICIENT IN:

RelativityOne

Nuix

LAW Prediscovery

Edit Pad Pro

Message Crawler

NetSuite

ReadySuite

**JOSHUA BURKE**

Senior Legal Technology Specialist

WORK EXPERIENCE**Avalon****Senior Legal Technology Specialist****September 2012 – Present**

- Manage, mentor, and develop team of four technicians, as well as assign and perform quality control for all projects
- Lead daily meetings to ensure processes remain on schedule
- Seek opportunities for development by mastering multiple pieces of software used in the realm of litigation
- **Awards and certifications include:** Relativity Certified Administrator, RelativityOne Review Pro, Review Management Specialist, Relativity Certified Administrator, RelativityOne Certified Pro, IPro Certified Administrator, IPRO Certified Trainer, Avalon Award of Excellence, Avalon Award, Professional Technical Services Team Member of the Year
- **Project examples:**
 - **Server Management/Data Retention Project:** This Q1 2022 organizational rock involved the identification of all data related to different matters and developing a way to purge all non-active client data. Additionally, the project scope was to report on how much data exists and which servers it exists. I owned the first few steps of this project starting with developing a new method of organization on our servers, rolling it out to my team for future work as well as going through and retrofitting this solution for all existing matters. This was a manual process of both updating folder structure as well as going through XML files used by Nuix to identify the evidence links and update these to reference the new structure. If this process was not handled with the most care it would cause the cases to break links and no longer function properly. After accomplishing this, I developed a method using Treesize on all appropriate servers and exporting out reports on each drive individually and then using Excel to manipulate this information with a combination of vlookups, pivot tables



JOSHUA BURKE

Senior Legal
Technology Specialist

LEARN MORE & FOLLOW

teamavalon.com

[Joshua on LinkedIn](#)

[Avalon on LinkedIn](#)

as well as other functions to get a aging client list and a file to load into NetSuite to properly bill our clients.

- **LAW Prediscovery Imaging:** This Q1 2022 project was to solve an issue where LAW Prediscovery would crash repeatedly during batch imaging jobs. I investigated the issue thoroughly and after discovering that it was being caused by outlook closing after imaging files and not reopening fast enough to image the next file, I wrote a batch file that would be used to launch LAW Prediscovery and would check repeatedly if Outlook was open. If Outlook was not open it would reopen the application. This batch script fixed the issue and we rolled the fix out to all of our stations.

Epic Systems Technical Services July 2011 – March 2012

- Solved time sensitive technical issues for Ochsner through determination and critical thinking skills.
- Prioritized incoming issues and time managed to direct and resolve incoming issues.
- Utilized effective interpersonal and leadership skills by regularly leading calls with client, creating outlines for projects, submitting summary of pertinent information, and delegating issues to the responsible parties.
- **Awards and certifications include:**
 - Epic MyChart Certified, Epic Ambulatory Certified, Epic Server Tech Camp Certified

EDUCATION

Utica College
August 2018 – December 2019
MS, Cybersecurity
Concentration in Cyber Operations

Grove City College
August 2009 – May 2011
BS, Mathematics

CONTACT

716.259.0254
joshua.burke@teamavalon.com

EXHIBIT A – Pricing Page
eDiscovery SaaS - (OT25112)

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1.1	Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	no cost	\$0.00
4.1.2	Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 7.00	\$ 700.00
4.1.7	Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	no cost	\$0.00
4.1.7.4	Contract Item #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	no cost	\$0.00
4.1.7.5	Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	no cost	\$0.00
4.1.7.7	Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.8	Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.7.6	Contract Item #8: Maintenance and Support Year 1	LS	1.00	no cost	\$0.00
4.1.1	Optional Renewal Year 2: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	no cost	\$0.00
4.1.2	Optional Renewal Year 2: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 7.00	\$ 700.00
4.1.7	Optional Renewal Year 2:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	no cost	\$0.00
4.1.7.4	Optional Renewal Year 2: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	no cost	\$0.00
4.1.7.5	Optional Renewal Year 2: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	no cost	\$0.00
4.1.7.7	Optional Renewal Year 2: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.8	Optional Renewal Year 2: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.7.6	Optional Renewal Year 2: Contract Item #8: Maintenance and Support Year 1	LS	1.00	no cost	\$0.00
4.1.1	Optional Renewal Year 3: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	no cost	\$0.00
4.1.2	Optional Renewal Year 3: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 7.00	\$ 700.00
4.1.7	Optional Renewal Year 3:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	no cost	\$0.00
4.1.7.4	Optional Renewal Year 3: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	no cost	\$0.00
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	no cost	\$0.00
4.1.7.7	Optional Renewal Year 3: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.8	Optional Renewal Year 3: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.7.6	Optional Renewal Year 3: Contract Item #8: Maintenance and Support Year 1	LS	1.00	no cost	\$0.00
4.1.1	Optional Renewal Year 4: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	no cost	\$0.00
4.1.2	Optional Renewal Year 4: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 7.00	\$ 700.00
4.1.7	Optional Renewal Year 4:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	no cost	\$0.00
4.1.7.4	Optional Renewal Year 4: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	no cost	\$0.00
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	no cost	\$0.00
4.1.7.7	Optional Renewal Year 4: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.8	Optional Renewal Year 4: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ 165.00	\$ 16,500.00
4.1.7.6	Optional Renewal Year 4: Contract Item #8: Maintenance and Support Year 1	LS	1.00	no cost	\$0.00
Total Cost					\$134,800.00

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.


Emily LaPane

3.4.25

Vendor Signature:

Date:

We intend to offer 4.1.1, 4.1.7, 4.1.7.4, 4.1.7.5 and 4.1.7.6 to the West Virginia Office of Technology for \$0, on a complimentary basis (as we customarily do not charge for these items as standard business practice and provide them inclusively). These are no-cost items, not no-bid items. The services will be provided free of charge.


	Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	State of West Virginia Centralized Request for Quote Info Technology

Proc Folder: 1619676 Doc Description: Cybersecurity e-Discovery Software as a Service (OT25112)			Reason for Modification:
Proc Type: Central Contract - Fixed Amt			
Date Issued 2025-02-06	Solicitation Closes 2025-02-26 13:30	Solicitation No CRFQ 0231 OOT2500000017	Version 1

BID RECEIVING LOCATION BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION 2019 WASHINGTON ST E CHARLESTON WV 25305 US
--

VENDOR Vendor Customer Code: VS0000048200 Vendor Name : Surge Avalon Holdings Inc Address : Street 1360 East 9th St , Suite 150 City : Cleveland State : OH Country : USA Zip . 44114 Principal Contact : Emily LaPane Vendor Contact Phone: 757.325.0911 Extension:
--

FOR INFORMATION CONTACT THE BUYER Toby L Welch (304) 558-8802 toby.l.welch@wv.gov

Vendor Signature X 	FEIN# 92-0441715	DATE 3.5.25
---	-------------------------	--------------------

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 US		WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON US	
	WV		WV

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

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description:

Please see the attached Exhibit A Pricing Page

Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 3:00 p.m.	2025-02-18

	Document Phase	Document Description	Page 3
OOT2500000017	Final	Cybersecurity e-Discovery Software as a Service (OT25112)	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

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.

(Printed Name and Title) Emily LaPane - Regional Account Executive eDiscovery Southeast
(Address) 5650 Breckenridge Parkway, Suite 103 Tampa, FL 33610
(Phone Number) / (Fax Number) 813.221.3266
(email address) emily.lapane@teamavalon.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract 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/Contract 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 this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; 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; 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.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Surge Avalon Holdings Inc

(Company) _____

(Signature of Authorized Representative) _____

Matthew Magill - Proposal Specialist 2.20.25

(Printed Name and Title of Authorized Representative) (Date)

315.471.3333

(Phone Number) (Fax Number)

matt.magill@teamavalon.com

(Email Address)

Revised 8/24/2023

ADDENDUM ACKNOWLEDGEMENT FORM

SOLICITATION NO.: CRFQ OOT2500000017

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 checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input checked="" 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.

Surge Avalon Holdings Inc

Company



Authorized Signature

3.4.25

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 8/24/2023

REQUEST FOR QUOTATION
e-Discovery Software as a Service

10 VENDOR DEFAULT: The following shall be considered a vendor default under this Contract.

- 10.1** Failure to perform Contract Services in accordance with the requirements contained herein.
- 10.2** Failure to comply with other specifications and requirements contained herein.
- 10.3** Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.
- 10.4** Failure to remedy deficient performance upon request.
- 10.5** The following remedies shall be available to Agency upon default:
 - 10.5.1** Immediate cancellation of the Contract.
 - 10.5.2** Immediate cancellation of one or more release orders issued under this Contract.
 - 10.5.3** Any other remedies available in law or equity.

11 MISCELLANEOUS:

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:	Emily LaPane
Telephone Number:	813.221.3266
Fax Number:	315.471.3334
Email Address:	emily.lapane@teamavalon.com

APPENDIX A:
SOFTWARE AS A SERVICE ADDENDUM

Begins on next page.

Version 11-1--19

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.

Version 11-1--19

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,

Version 11-1--19

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

Version 11-1--19

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.

Version 11-1--19

- 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

Version 11-1--19

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

Version 11-1--19

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

Version 11-1--19

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

Version 11-1--19

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:

- a. Access and use the service for its business purposes;
- b. For SaaS, use underlying software as embodied or used in the service; and
- c. 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.

Version 11-1--19

AGREED:

Name of Agency: _____

Signature: _____

Title: _____

Date: _____

Name of Vendor Surge Avalon Holdings IncSignature:  _____Title: Proposal SpecialistDate: 2.20.25

Version 11-1--19

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.)

Surge Avalon Holdings Inc

Name of Service Provider/Vendor: _____

State of West Virginia


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: Emily LaPane
Email address: emily.lapane@teamavalon.com
Phone Number: 757-325-0911

	Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	State of West Virginia Centralized Request for Quote Info Technology

Proc Folder: 1619676 Doc Description: Addendum No 1 Cybersecurity e-Discovery SAAS (OT25112)			Reason for Modification: Addendum No 1 is issued to modify the bid opening date
Proc Type: Central Contract - Fixed Amt			
Date Issued	Solicitation Closes	Solicitation No	Version
2025-02-24	2025-03-05 13:30	CRFQ 0231 OOT2500000017	2

BID RECEIVING LOCATION BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION 2019 WASHINGTON ST E CHARLESTON WV 25305 US
--

VENDOR			
Vendor Customer Code: VS0000048200 Vendor Name : Surge Avalon Holdings Inc Address : Street : 1360 East 9th St , Suite 150 City : Cleveland State : OH Country : USA Zip : 44114 Principal Contact : Emily LaPane Vendor Contact Phone: 757.325.0911 Extension:			

FOR INFORMATION CONTACT THE BUYER Toby L Welch (304) 558-8802 toby.l.welch@wv.gov

Vendor Signature X 	FEIN# 92-0441715	DATE 3.5.25
---	-------------------------	--------------------

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

ADDITIONAL INFORMATION
Addendum No 1 is issued for the following reasons:
1) 1) To modify the bid opening date from 2/26/25 to 3/5/25.
--no other changes--

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US

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

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description:

Please see the attached Exhibit A Pricing Page


Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.

SCHEDULE OF EVENTS		
<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 3:00 p.m.	2025-02-18

	Document Phase	Document Description	Page 3
OOT2500000017	Final	Addendum No 1 Cybersecurity e-Discovery SAAS (OT25112	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

	Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	State of West Virginia Centralized Request for Quote Info Technology

Proc Folder: 1619676 Doc Description: Addendum No 2 Cybersecurity e-Discovery SAAS (OT25112)		Reason for Modification: Addendum no 2 is issued to publish questions and answers and to modify the bid opening date.
Proc Type: Central Contract - Fixed Amt		
Date Issued 2025-03-03	Solicitation Closes 2025-03-07 13:30	Solicitation No CRFQ 0231 OOT2500000017
		Version 3

BID RECEIVING LOCATION BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION 2019 WASHINGTON ST E CHARLESTON WV 25305 US
--

VENDOR			
Vendor Customer Code: VS0000048200 Vendor Name : Surge Avalon Holdings Inc Address : Street : 1360 East 9th St , Suite 150 City : Cleveland State : OH Country : USA Zip : 44114 Principal Contact : Emily LaPane Vendor Contact Phone: 757.325.0911 Extension:			

FOR INFORMATION CONTACT THE BUYER Toby L Welch (304) 558-8802 toby.l.welch@wv.gov

Vendor Signature X 	FEIN# 92-0441715	DATE 3.5.25
---	-------------------------	--------------------

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

ADDITIONAL INFORMATION

Addendum No 2 is issued for the following reasons:

- 1) To Publish Vendor questions with the Agency's responses.
- 2) To modify the bid opening date from 3/5/25 to 3/7/25.

--no other changes--

INVOICE TO				SHIP TO			
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US				WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US			

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

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description:

Please see the attached Exhibit A Pricing Page

Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 3:00 p.m.	2025-02-18

	Document Phase	Document Description	Page 3
OOT2500000017	Final	Addendum No 2 Cybersecurity e-Discovery SAAS (OT25112	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

If you have any questions or concerns, please contact:

Emily LaPane

Regional Account Executive
eDiscovery Southeast
Surge Avalon Holdings Inc

emily.lapane@teamavalon.com

5650 Breckenridge Parkway, Suite 103
Tampa, FL 33610

www.teamavalon.com

Thank you!



Syracuse
315.471.3333

Rochester
585.242.9999

Buffalo
716.995.7777

Cleveland
216.592.9999

Tampa
813.221.3266

Omaha
402.885.8800

Detroit
248.955.9200

Phoenix
602.975.4001

eDiscovery | Litigation Support | Document Scanning | Printing and Copying | Design-Build Printing | Bid Management

CERTIFICATE *of* SIGNATURE

REF. NUMBER
HIZL6-K5XOL-9WDNC-QCV4C

DOCUMENT COMPLETED BY ALL PARTIES ON
06 MAR 2025 16:56:27 UTC

SIGNER

EMILY LAPANE

EMAIL
EMILY.LAPANE@TEAMAVOLON.COM

TIMESTAMP

SENT
06 MAR 2025 16:56:27 UTC

SIGNED
06 MAR 2025 16:56:27 UTC

SIGNATURE

Emily LaPane

IP ADDRESS
209.122.120.180

LOCATION
NEW YORK, UNITED STATES

