

Securely Managed

Bibb County Public Schools
SEIM/SOC/XDR Solution
RFP # 26-005

August 25, 2025

131 Guilford Road, Bloomfield Hills, MI 48304
Office (248) 723-5224 Fax (866) 531-8620
www.securelymanaged.com
DUNS – 117302668
EIN – 82-2440108
Point of Contact: Sajay Rai
Email: sajayrai@securelymanaged.com

August 25, 2025

Attn: Ms. Elaine M. Wilson-Beverly
Procurement Director
Bibb County School District
4580 Cavalier Drive
Macon, Georgia 31220

Dear Ms. Wilson-Beverly,

Securely Managed LLC ("SM") is delighted to present this response to assist the Bibb County School District with their SEIM/SOC/XDR solution referenced in RFP #26-005. Securely Managed was officially formed in 2017 as a separate and independent company from its sister company, Securely Yours LLC, to provide security operation services to our clients. Our SOC is a 24x7x365 service operated within the United States and staffed entirely by U.S.-based employees. SM provides Managed Security Services that include SIEM implementation and monitoring, SOC-as-a-Service (SOCaaS), Endpoint Detection and Response (EDR) implementation and monitoring, continuous vulnerability management, penetration testing, and patch management.

We have extensive experience in K–12 environments, most notably through our recent win with Kansas City Public Schools in State of Missouri under the Cybersecurity Pilot Program from FCC/USAC. In addition, we currently provide MDR services to Oakland Schools (all the field and non-field schools within Oakland County in Michigan). We have also provided MDR services to Washington County Public Schools in the State of Maryland and Midview public schools in the State of Ohio.

This background ensures we understand the unique scale, resource constraints, and regulatory obligations facing Bibb County School District. We are delighted about the possibility of working together and are confident that our team and approach can exceed the value you expect. As you review this proposal, we would like to draw your attention to a few key points that demonstrate the experience and value we bring to BCSD, and why our clients feel that SM is the best choice as a security company:

- **Top 250 MSSP Provider in the world –** SM is listed in MSSP Alert's 2023 list as one of the top 250 Managed Security Service Providers (MSSPs) worldwide. SM has maintained a position in the MSSP Alert top 250 for the past five straight years.

- **Experienced personnel –** Many MSSP providers come from a Managed Service Provider (MSP) background. In contrast, our roots are in cyber consulting. Our team of professionals has extensive security and industry experience, supported by relevant certifications (CISSP, CISA, CISM), and significant "white hat" expertise. By engaging SM, BCSD will have access to the best security specialists available - professionals with creative ideas to strengthen your security program and help resolve cyber incidents faster.

- **Methodologies and tools –** We have developed a repeatable and proven methodology, informed by our consulting experience. From robust assessment and architecture design methodologies to specialized security tools, our approach increases efficiency, reduces project costs and duration, and helps us isolate the root cause of any cyber incident quickly.

- **Unique Services –** SM is a pioneer in developing new and creative security services for our clients. One example is our Virtual (or temporary) Chief Information Security Officer (vCISO) service, originally offered in 2010 and still used by numerous clients today. We also develop mobile apps to support our clients' security management efforts, ensuring that we remain at the forefront of cyber innovation and keep BCSD abreast of the latest solutions.

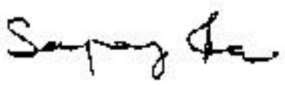
- **Regulatory knowledge –** We are well-versed in various regulatory and industry requirements, including ISO, NIST, PCI, and HIPAA. Our approach confirms that the results of vulnerability testing conform to these standards and best practices.

- **From Thought to Finish –** Our professionals are not only experienced in providing high-level recommendations for improving an information security program, but can also manage the proper implementation of those solutions. We remain available for periodic counsel and guidance to ensure that our recommendations achieve the desired results.

- **Incident Response –** We have decades of experience assisting clients during and after data breaches, swiftly deploying security processes and procedures to address any gaps in their security posture.

Thank you for giving us the opportunity to respond to this RFP. We look forward to working with you and your team at BCSD.

Securely Yours,



Sajay Rai
CEO & President
Securely Managed LLC
(248) 723-5224
sajayrai@securelymanaged.com

Table of Contents

SIEM Solution and BCSD Requirements *5*
SOC Solution and BCSD Requirements *7*
Securely Managed SOC Services 7
Specific BCSD Requirements – SOC 7
Extended Detection & Response – XDR *8*
Specific BCSD Requirements — XDR 8
Company Background *9*
Experience *11*
Cost *12*
Experience with Erate *13*
Submittal Forms *15*
Certification Letter 15
Contractor Affidavit - Notarized 16
Certificate Regarding Debarment, Suspension, Ineligibility 17
Non-Collusion Affidavit 18
Offeror Affirmation Form 19
Certificate of Non-Collusion 20

SIEM Solution and BCSD Requirements

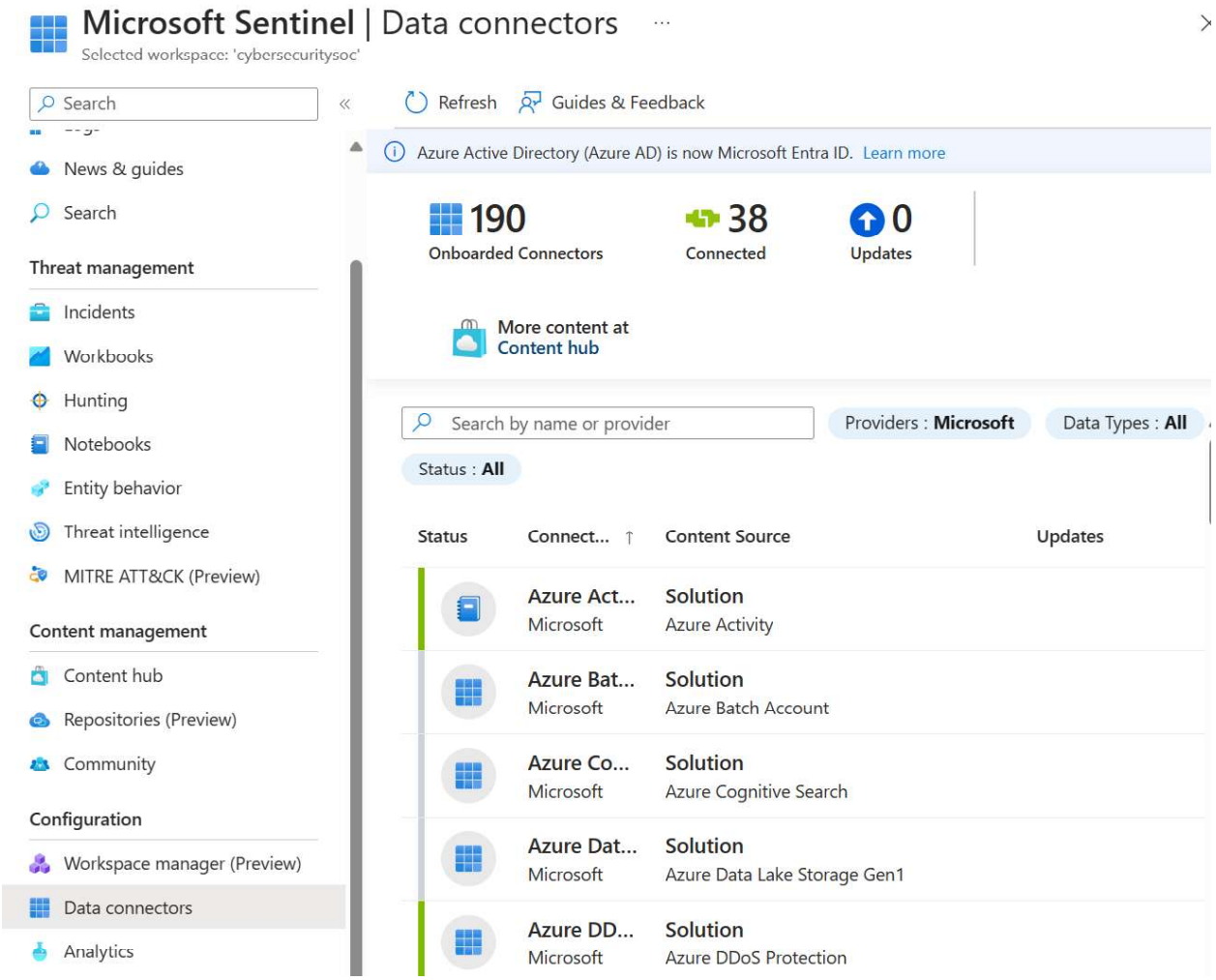
As BCSD already has deployed a SIEM solution (Microsoft Sentinel), Securely Managed will provide the following services as outlined in the RFP requirements:

SOC to include full SIEM capabilities for customers 24x7.
SM's Security Operations Center (SOC) will provide 24x7x365 services to manage, configure, monitor and report using BCSD Microsoft Sentinel deployment.

Must include data aggregation, correlation, threat detection and incident response
SM SOC will configure the current BCSD Microsoft Sentinel for data aggregation, correlation, threat detection and incident response. Specifically, SM will provide support for:

Data Ingestion and Normalization
SM will onboard the district's data into our Microsoft Sentinel workspace, and use data connectors to start ingesting your data. Microsoft Sentinel comes with many out of the box connectors for Microsoft services, which integrate in real time. For example, the Microsoft Defender XDR connector is a service-to-service connector that integrates data from Office 365, Microsoft Entra ID, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps.

Built-in connectors enable connection to the broader security ecosystem for non-Microsoft products. For example, use Syslog, Common Event Format (CEF), or REST APIs to connect your data sources with Microsoft Sentinel.



Advanced Threat Detection

AI & Machine Learning: Our SOC analysts leverage automated correlation and anomaly detection powered by Microsoft's global threat intelligence.

Threat-Based Recommendations: Identify coverage gaps for specific attack vectors (e.g., Ransomware, Business Email Compromise).

Security Orchestration, Automation, and Response (SOAR)
Logic Apps and Playbooks (SOAR capabilities) are a core part of Azure Sentinel's automation framework. Although not strictly mandatory, Logic Apps are instrumental in enhancing your security operations:

- **Orchestration of Workflows:** Automate repetitive tasks (e.g., open a ServiceNow ticket, and send notifications to Teams).
- **Cross-Platform Integration:** Connect your cloud platforms (AWS, GCP) and business tools (Salesforce, ServiceNow, Jira) within a single workflow.
- **Scalable Response:** Establish incident response playbooks for rapid containment of threats (e.g., quarantine an endpoint, or block an IP at the firewall).
- **Customizable Templates:** Reusable, community-driven Logic App templates available on GitHub for quick deployment.

By embedding Logic Apps into Azure Sentinel, organizations achieve faster mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR), significantly reducing the impact of cyber threats.

Threat Hunting and Investigation
SM will review the information provided through threat intelligence feeds from Sentinel and other sources, interpret and investigate that intelligence data which applies specifically to BCSD's environment. SM will also work with BCSD's team to remediate the impact of those threats on the environment.

Monitoring & Reporting
Sentinel's Workbook engine lets our SOC build live, role-based dashboards—tactical views for analysts (alert queues, connector health) and executive summaries for district leadership (MTTD, MTTR, top use-cases). Analytics rules merge related alerts into a single incident, driving down false positives by 60–70 percent. Monthly compliance packs map detections and controls to FERPA, CIPA and NIST CSF functions, giving BCSD board-ready evidence without extra tooling.

Support & Services
Our US-based SOC monitors the environment 24 × 7 × 365 and has direct escalation into Microsoft Premier Support for high-severity platform issues. During onboarding we run two half-day training sessions covering KQL, dashboard editing and playbook approval, and we hand over a hard-copy "Sentinel Runbook" that documents every connector, rule and SLA in plain language.

Security & Compliance
All log traffic is encrypted using TLS 1.2+; data rests in Azure Storage with platform-managed keys or optional customer-managed keys. Granular RBAC roles (Reader, Responder, Contributor) restrict what analysts, administrators and auditors can do, and every action—query, rule change, playbook run—is captured in Sentinel's immutable audit log for later review.

SOC Solution and BCSD Requirements

Securely Managed SOC Services

SM has been operating 24x7x365 virtual Security Operations Center (SOC) since 2017. The entire SOC infrastructure and personnel is based in United States, and no client information ever leaves US. SM resources work exclusively for SM and no portion of the service is outsourced to sub-contractors and 3rd party vendors (besides the licensing of USM Anywhere through LevelBlue).

SM's SOC by default includes but is not limited to the following services:

- 24x7 monitoring with a human capable of neutralizing threats immediately
- Log aggregation, automated parsing, coupled with human eyes on a SIEM
- Create operational playbook (run books) and escalation procedures
- Notification of alarms within the agreed upon Service Level Agreements (SLAs), usually within 15 minutes
- Daily (within 24 hours) and Monthly (within 30 days) reporting
- Monthly meetings with the client
- Custom configuration of USM Anywhere
- Custom rules
- Modification of current rules
- Monitoring the usage of storage
- Assist in ingesting log of new technologies deployed by the client
- Ensuring the critical assets are ingesting logs
- Monitoring the sensors and the connection to USM Anywhere
- Training for client personnel on use of USM Anywhere, custom reporting and SOC services

Specific BCSD Requirements – SOC

Network & DNS Visibility
We ingest and monitor endpoint telemetry together with north/south and east/west network flows and DNS resolver logs across all schools to identify lateral movement, command-and-control, and domain abuse.

Deception / Honeypots
SM will deploy multiple layers of deception—e.g., service decoys, credential traps, and honey-shares—in key segments. Deception events feed the SIEM in real time for analyst validation and rapid response.

Hosting & Data Residency (AWS U.S.)
The service is hosted in AWS U.S. regions (or AWS-equivalent) with full redundancy and a U.S. backup datacenter. All customer support and security analysts are U.S.-based.

Access & Notifications (Web • Mobile • Chat • Phone)
District staff receive immediate 24/7 access to live analysts via web console, mobile app (with push), in-app chat, and a staffed hotline; escalations follow runbooks and on-call contact trees.

Role-Based Access for District Leadership
We provision role-based accounts for all IT Directors and an executive dashboard + priority line for the CEO, available 24×7.

Compliance & Threat Intelligence
Our SOC operates under SOC 2 Type II controls and fuses multiple DoD-class threat-intel feeds alongside commercial and community sources (including OTX) to enrich correlation rules and detections.

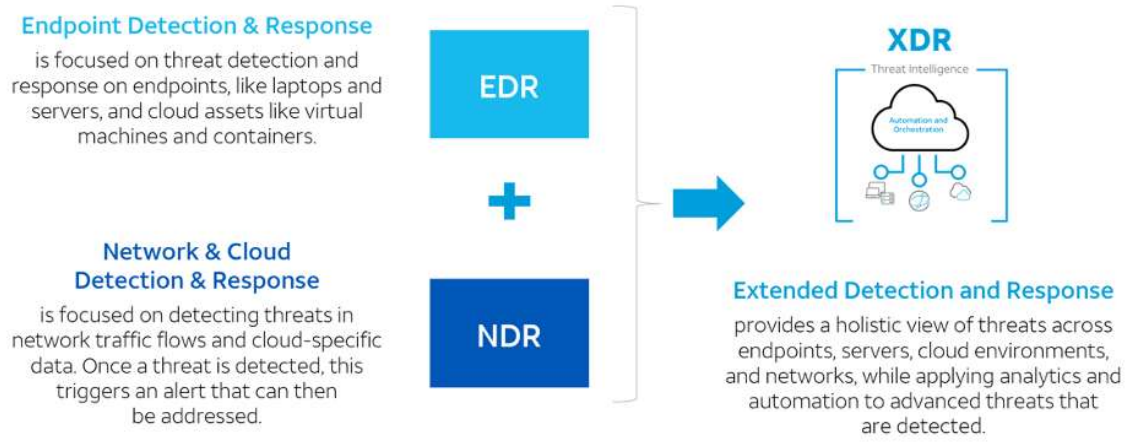
Annual External Penetration Test (Up to 1,000 IPs)
The subscription includes one external penetration test annually covering up to 1,000 public IPs, with findings triaged in the SOC and tracked to closure.

Reporting (Custom PDF Deliverables)
Beyond dashboards, SM provides custom, scheduled PDF reports (monthly and ad-hoc) pulled directly from the SOC console, including trends, MITRE mapping, and ticketing SLAs.

CISO-as-a-Service
BCSD is assigned a U.S.-based CISO who is available 24×7 for major incidents and provides governance sessions (quarterly or as needed), policy guidance, tabletop exercises, and board-level briefings.

Extended Detection & Response – XDR

The detection and response industry are continuously evolving, and the current trend is to have a holistic view of threats across endpoints, servers, cloud environments and network, while applying analytics and automation to advanced threats that are detected. This in essence is the definition of Extended Detection and Response or XDR. It is accomplished through the feeds provided by the Endpoint Detection and Response (EDR) – which is focused on threat and detection/response on endpoints and Network & Cloud Detection & Response (NDR) – which is focused on detecting threats in network traffic flows and cloud-specific data. This relationship is shown in the diagram below:



By integrating the feeds from EDR and NDR and providing continuous monitoring through single pane of glass, SM can assist BCSD to utilize Microsoft Sentinel as the XDR solution

Specific BCSD Requirements — XDR

- **Ransomware & Data-Exfiltration Controls (Servers).** We will enforce behavior-based protections that stop encryption activity, terminate malicious processes, and prevent unsanctioned outbound transfer of sensitive data across physical and virtual servers. Post-event rollback and outbound-block rules are included, with incident evidence retained in the case record.
- **AI-Driven Endpoint Protection with After-Hours Containment.** Endpoints and servers use an AI/ML prevention engine for exploits, malware, and lateral-movement behaviors. After hours, the SOC is authorized to isolate a device from the network when confidence/risk thresholds are met, preserving management channels for investigation and recovery.
- **SOC-Configured & Managed.** XDR policies, profiles, exclusions, upgrades, and tuning are owned and maintained by SM. All detections, actions, and tuning changes are tracked in the SOC case system and reflected in monthly reports.
- **Full SOC/SIEM Integration.** XDR telemetry (endpoint, server, network, and cloud) is ingested into Microsoft Sentinel, correlated with identity/asset/vulnerability context, and managed through one case and dashboard experience by our 24×7 U.S.-based analysts.
- **After-Hours Monitoring for the District.** The SOC monitors and manages the AI engine after hours for BCSD, following your on-call tree and escalation thresholds defined in jointly approved runbooks.
- **Deliverables.** Monthly XDR PDFs summarize prevented ransomware/exfil attempts, isolated devices, response times, and MITRE ATT&CK coverage; ad-hoc reports are available from the SOC console.

Company Background

Securely Managed was officially formed in 2017 as an independent entity, separating from its sister company, Securely Yours LLC. The goal was to provide focused and specialized security operations services to a growing client base. Our firm is privately owned and led by a team of cybersecurity experts with deep industry experience. SM specializes in Managed Security Services, including SIEM implementation and monitoring, SOC-as-a-Service (SOCaaS), Endpoint Detection and Response (EDR), continuous vulnerability management, penetration testing, and patch management.

Our leadership team consists of experienced professionals, all of whom bring a wealth of security consulting and operational knowledge to the firm. The core team is comprised of Certified Information Systems Security Professionals (CISSP), Certified Information Security Managers (CISM), and other key industry certifications. The organization is structured to deliver effective and efficient security services through our in-house security operations center (SOC) and our extended teams, who specialize in customized security solutions.

Our Team

Sajay Rai – Project and Account Executive



Sajay Rai has more than 30 years of experience in information technology, specializing in information security, business continuity, privacy, IT audit and information risk. Mr. Rai is the Founder and CEO of Securely Yours LLC. Securely Yours LLC is focused on delivering innovative solutions through delivery channels like Software-as-a-Service, Managed Services and traditional IT consulting. Mr. Rai's clients are in the financial, manufacturing, retail, healthcare and utility industry.

Prior to starting Securely Yours LLC, Mr. Rai was a Partner with Ernst & Young LLP for 10 years and was responsible for the information advisory practice in the Detroit Metro area. He also served as the national leader of EY's Information Security practice. Mr. Rai's clients included General Motors, Blue Cross Blue Shield of Michigan, Yazaki North America, Tecumseh and Federal Mogul. He also served as a member of his firm's Partners Advisory Council.

Mr. Rai also worked with IBM for 13 years, most recently serving as an executive of the national Business Continuity and Contingency consulting practice. He was instrumental in starting the company's Information Security consulting practice and managing its information technology consulting practice in Latin America.

Mr. Rai co-authored a recently published book, "Defending the Digital Frontier – A Security Agenda", which guides business and IT executives on how to develop an effective and efficient information security program within their enterprise. He also led the publication of Institute of Internal Auditors' (IIA) Global Technology Audit Guide (GTAG) No. 9 on the topic of Identity and Access Management.

Mr. Rai serves on the board of ISACA Detroit Chapter and Society of Information Management (SIM) Detroit Chapter. Mr. Rai also is on the advisory boards of Walsh College's Accounting Advisory Committee, Oakland University's Cyber Committee and Wayne State's IT council. Mr. Rai is a regular speaker at industry conferences on information security, business continuity, technology strategy and is frequently quoted in magazines and newspapers. He has also served as expert witness in litigation cases in the area of information security.

He holds a master's degree in information management from Washington University of St. Louis, and a bachelor's degree in computer science from Fontbonne College of St. Louis.

Philip Chukwuma CISSP – Principal MSSP Architect and Project Manager



The project team also comprises of our Chief Technology Officer, Philip Chukwuma. He has over 20 years of experience in Information Technology, information security, privacy and business continuity. His expertise is in the area vulnerability and risk management, security engineering, mobile security, Identity and Access Management, network architecture, disaster recovery planning, and security architecture.

Prior to joining Securely Yours, Mr. Chukwuma was with Ernst & Young LLP as a Manager in the Risk Advisory practice. He worked on several engagements in IT Security, Identity and Access Management, ERP Integrity, SAP Security, Segregation of Duties (SOD), and Infrastructure Management (Problem, Incident, Change, Event Management, Active Directory, UNIX, etc.).

During his career, Mr. Chukwuma has led several engagements as an Architect where he has invented ideas to streamline the implementation of security solutions. He has designed several solutions in the areas of databases, routers and switches, virtualized environment and IAM.

Philip received a bachelor's degree from the University of North Texas in Denton, and his M.B.A. from the same University. Philip is a CISSP.

Richard Cozart – Senior MSSP Architect and Co-Project Manager



Richard Cozart is the Chief Mobility Officer with Securely Yours LLC. He specializes in developing and evaluating secure solutions for mobile and web technologies. He also developed multiple mobile applications for the android and Apple's IOS Platform.

Richard is our lead MSSP Architect. In his role during the initial MSSP deployment, he works with the client's IT infrastructure, network and cloud system groups to ensure that the appropriate logs are ingested, parsed and analyzed by the SIEM software. He ensures that the API interfaces are working properly and if needed, writes code for custom APIs. As his support role for MSSP services, Richard reviews the alarms for severity and provides consultation to the clients on how to handle the alarms. He also customizes, updates and maintains the rules written for each client and supports our SOC team with requirements of customized reporting and rule writing.

Prior to joining Securely Managed, Richard was a software engineer for Accenture and co-founder of the web solutions firm, A-Z computers. Richard received a bachelor's degree from Eastern Michigan University, with a major in computer information systems.

Michael Staley – SOC Director



Michael is the SOC Director with Securely Managed. Michael has been with Securely Managed since 2018 and started as a SOC Analyst. Michael has a strong operations and cybersecurity background. He manages all aspects of Securely Managed's MSSP SOC Operations, including the personnel, technical and client communication. His technical abilities include the reviewing of SIEM alarms, triaging the events/alarms, writing SIEM rules and customizing reports for the clients.

Michael has tremendous and proven ability to collaborate with executives to identify areas of improvement for cyber monitoring. He can also work at a technical level with the clients and implement incident response solutions. With his experience with next generation software like Power BI, he can customize reports for our clients.

Michael graduated from Oakland University with his Bachelor of Science in Management Information Systems and a minor in Information Security Management. He has also completed an 8-week Cybersecurity Fellowship at Carnegie Mellon University, where he studied and worked with instructors and practitioners from US-Cert in their lab at the internationally renowned Software Engineering Institute.

Experience

SM has extensive experience performing services like those requested by Bibb County School District, including SIEM implementation, 24×7 SOC monitoring, and rapid incident response. Our methodology is built on repeatable, proven processes that have been implemented across various K–12 and public-sector institutions, ensuring consistency and reliability. We are familiar with the latest regulatory requirements in a K–12 environment, such as data privacy mandates, and incorporate these standards into our security solutions.

Just last month, we were awarded the SIEM and SOAR service by Kansas City Public Schools in Missouri. This engagement is based on FCC/USAC E-rate cyber pilot program. In addition, Securely Managed has or is servicing these K-12 schools:

Client 1:

Organization Name:	Oakland Schools
Address:	2111 Pontiac Lake Road, Waterford, MI 48328
Contact Person:	Christopher Hammond
Phone #:	(248) 209-2153
Email:	Christopher.hammond@oakland.k12.mi.us
Project Dollar:	Over $200,000 per year.
Services Provided:	24x7x365 SIEM and SOC Monitoring. Services include incident response, threat intelligence and hunting, customized reporting and new technology support. Services scope includes the 14 field school districts and 7 of the 14 non-field school districts.

Client 2:

Organization Name:	Washington County Public Schools
Address:	10435 Downsville Pike, Hagerstown, MD 21740
Contact Person:	Christine Moats
Phone #:	301-766-2873
Email:	moatchri@wcps.k12.md.us
Project Dollar:	Over $100,000 per year.
Services Provided:	24x7x365 SIEM and SOC Monitoring. Services include incident response, threat intelligence and hunting, customized reporting and new technology support. Services scope includes the entire WCPS.

Client 3:

Organization Name:	Midview Ohio Schools
Address:	260 S State St. #932 Westerville OH 43086
Contact Person:	John LaPlante
Phone #:	(330) 881-1661
Email:	jlaplante@vinsonedu.com
Project Dollar:	Less than $50,000 per year.
Services Provided:	24x7x365 SIEM and SOC Monitoring. Services include incident response, threat intelligence and hunting, customized reporting and new technology support.

In addition, SM currently services other State and Local agencies and can provide contact information upon request:

- State of Michigan – Office of Auditor General
- State of Maryland – State Board of Elections

Cost

The following cost is based on the following assumptions:

1. Microsoft Sentinel is licensed by BCSD and Securely Managed is providing the SOC and Managed Detection and Response services.
2. The licensing, support and maintenance costs, including the storage and compute power for Microsoft Sentinel, are paid by BCSD.
3. The number of IPs for penetration testing is not to exceed 1000 IPs.

Requested Services	Total Amount of Bid
1. SIEM Services	Included in SOC Services
2. SOC Services	$72,000.00
3. XDR Services	Included in SOC Services
4. Penetration Testing Services – 1000 IPs	$26,000.00
Total for One Year	$98,000.00
Grand Total for Three Years	$294,000.00

Experience with Erate

SM is an approved service provider with FCC and is in good standing. The FRN number is shown in this screen shot (Sajay Rai, as sole proprietor and DBA Securely Managed). The FRN number is 0034937672.



You registered FRN **0034937672** on **February 18 2024 10:53 PM**.
Your registration information was last updated on **February 18 2024 10:53 PM**.

Update a Domestic Individual

Salutation:	Mr	First Name:*	Sajay
Middle Initial:		Last Name:*	Rai
Suffix:		Doing Business As:	Securely Managed LLC
SSN:	*****0875		

Please enter a New SSN and Confirm New SSN if you wish to update your FRN's Social Security Number or Taxpayer Identification Number. You may only use this form to correct an error in the FRN. This form CANNOT be used to notify the FCC of changes in ownership of spectrum licenses. Changes in ownership of spectrum licenses must be filed with the appropriate FCC Bureau responsible for the particular license.

New SSN:		Confirm New SSN:	

Contact Information

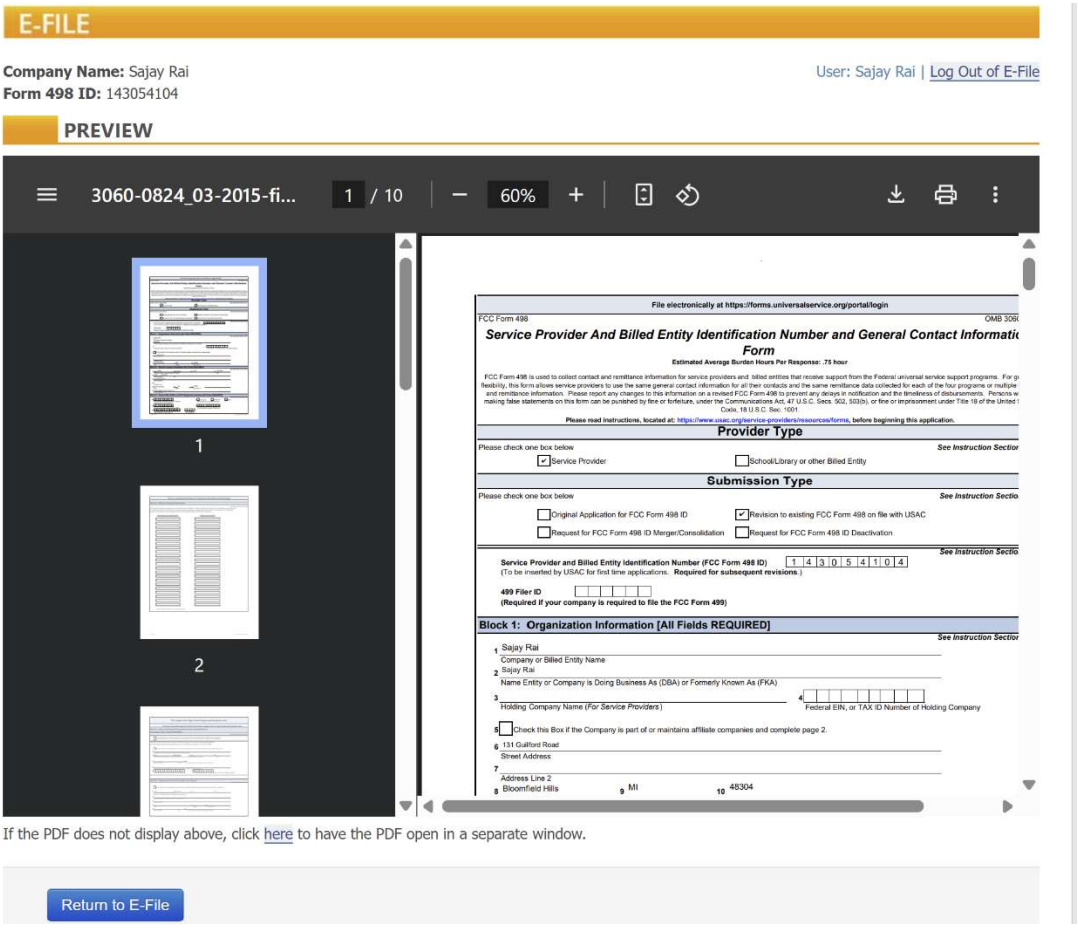
Same as Above:	☐		
Organization:		Position:	
Salutation:	Mr	First Name:*	Sajay
Middle Initial:		Last Name:*	Rai
Suffix:			
Address Line 1:*	131 Guilford Road	Address Line 2:	
City:*	Bloomfield Hills	State:*	MICHIGAN
Zip Code: *	48304	Phone:	248 723 5224 ext.
Fax:		Email:*	sajayrai@securelymanagec

SUBMIT Go Back

Asterisks (*) indicate required fields.

Revised: April 2005 Form 161 - Approved by OMB 3060-0917

The SPIN number from USAC site is 143054104. The screen shot from USAC site is shown below.



E-FILE

Company Name: Sajay Rai
Form 498 ID: 143054104

User: Sajay Rai | Log Out of E-File

PREVIEW

3060-0824_03-2015-fi... 1 / 10 60%

File electronically at https://forms.universalservice.org/portal/login

FCC Form 498 OMB 3060

Service Provider And Billed Entity Identification Number and General Contact Information Form

Estimated Average Burden Hours Per Response: .75 hour

Please read instructions, located at: https://www.usac.org/service-providers/resources/forms, before beginning this application.

Provider Type

Please check one box below — See Instruction Section

☑ Service Provider ☐ School/Library or other Billed Entity

Submission Type

Please check one box below — See Instruction Section

☐ Original Application for FCC Form 498 ID ☑ Revision to existing FCC Form 498 on file with USAC

☐ Request for FCC Form 498 ID Merger/Consolidation ☐ Request for FCC Form 498 ID Deactivation

Service Provider and Billed Entity Identification Number (FCC Form 498 ID) 1 4 3 0 5 4 1 0 4

(To be inserted by USAC for first time applications. Required for subsequent revisions.)

499 Filer ID

(Required if your company is required to file the FCC Form 499)

Block 1: Organization Information [All Fields REQUIRED]

See Instruction Section

1 Sajay Rai — Company or Billed Entity Name

2 Sajay Rai — Name Entity or Company is Doing Business As (DBA) or Formerly Known As (FKA)

3 Holding Company Name (For Service Providers) 4 Federal EIN, or TAX ID Number of Holding Company

5 ☐ Check this Box if the Company is part of or maintains affiliate companies and complete page 2.

6 131 Guilford Road — Street Address

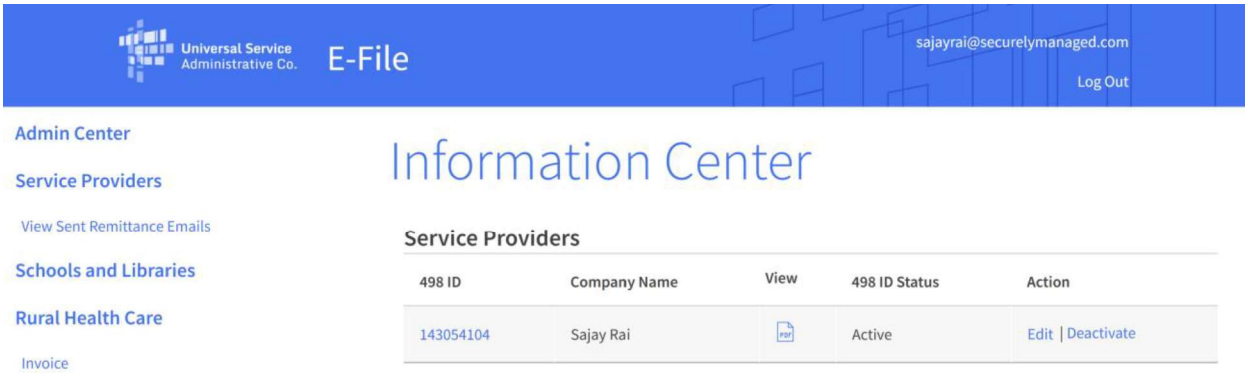
7 Address Line 2

8 Bloomfield Hills 9 MI 10 48304

If the PDF does not display above, click here to have the PDF open in a separate window.

Return to E-File

In addition, SM is in active status as shown on the USAC website:


Universal Service Administrative Co.
E-File
sajayrai@securelymanaged.com
Log Out
Admin Center
Service Providers
View Sent Remittance Emails
Schools and Libraries
Rural Health Care
Invoice
Information Center
Service Providers
498 ID
Company Name
View
498 ID Status
Action
143054104
Sajay Rai
Active
Edit | Deactivate

Submittal Forms

Certification Letter

BIBB COUNTY SCHOOL DISTRICT

ATTACHMENT A
Certification Letter
(Form must be completed and returned with bid.)

I certify that I have read and understand the terms and conditions herein. I further state that I am and/or my company is capable, able to, and will provide the requested product(s) and/or service(s) described herein. I am the owner or agent of the company stated below and am authorized and empowered to contract. By my signature on this RFQ, I/we guarantee and certify that all items included in my bid meet or exceed specifications.

I certify that this bid is made without prior understanding, agreement, or connection with any corporation, firm or person submitting a bid for the same materials, supplies, equipment, or services and is in all respects fair and without collusion or fraud. I understand collusive bidding is a violation of State and Federal Law and can result in fines, prison sentences, and civil damage awards. I agree to abide by all conditions of this RFQ and certify that I am authorized to sign this bid for the Contractor.

SUBMITTED BY Sajay Rai DATE 08-18-2025

TITLE President & CEO EMAIL: sajayrai@securelymanaged.com

COMPANY NAME Securely Managed LLC

ADDRESS 131 Guilford Rd CITY Bloomfield Hills ST MI ZIP 48304

TELEPHONE NUMBER 248-723-5224 FAX NUMBER 866-531-8620

COMPANY WEBSITE www.securelymanaged.com

SIGNATURE Sajay Rai

DO YOU ACCEPT VISA? No

ADDITIONAL FEE IF PAYMENT MADE WITH VISA: NA

Contractor Affidavit - Notarized

BIBB COUNTY SCHOOL DISTRICT

ATTACHMENT B

Contractor Affidavit under O.C.G.A. § 13-10-91(b)(1)

By executing this affidavit, the undersigned contractor verifies its compliance with O.C.G.A. § 13-10-91, stating affirmatively that the individual, firm or corporation which is engaged in the physical performance of services on behalf of Bibb County School District has registered with, is authorized to use and uses the federal work authorization program commonly known as E-Verify, or any subsequent replacement program, in accordance with the applicable provisions and deadlines established in O.C.G.A. § 13-10-91. Furthermore, the undersigned contractor will continue to use the federal work authorization program throughout the contract period and the undersigned contractor will contract for the physical performance of services in satisfaction of such contract only with subcontractors who present an affidavit to the contractor with the information required by O.C.G.A. § 13-10-91(b). Contractor hereby attests that its federal work authorization user identification number and date of authorization are as follows:

82-2440108
Federal Work Authorization User Identification Number

August 2017
Date of Authorization

Securely Managed
Name of Contractor

Name of Project SIEM/SOC/XDR

Securely Managed
Name of Public Employer

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on 18th, Aug 2025 in Bloomfield Hills (city), MI (state).

Sajay Rai
Signature of Authorized Officer or Agent

SAJAY RAI
Printed Name and Title of Authorized Officer or Agent

SUBSCRIBED AND SWORN BEFORE ME
ON THIS THE 18th DAY OF August, 2025.

NOTARY PUBLIC

My Commission Expires:
April 1, 2031

CONSUELA MAYS
Notary Public - State of Michigan
County of Wayne
My Commission Expires Apr 1, 2031
Acting in the County of Oakland

Certificate Regarding Debarment, Suspension, Ineligibility

BIBB COUNTY SCHOOL DISTRICT

ATTACHMENT C

Certificate Regarding Debarment, Suspension, Ineligibility
(Form must be completed and returned with bid.)

The Bibb County School District is a recipient of Federal monies. As such we require that participating vendors not be debarred, suspended, ineligible or excluded from doing business with the Federal government or any agency thereof.

The prospective participant certifies, by submission of the bid, that neither it, nor its principals, is presently debarred, suspended, proposed for debarment, declared ineligible, or excluded from participation in this transaction by any Federal department or agency.

Securely Managed LLC
Organization Name

Sajay Rai - President & CEO
Name(s) and Title(s) of Authorized Representative(s)

Sajay Rai — 08-18-2025
Signature(s) — Date

Non-Collusion Affidavit

BIBB COUNTY SCHOOL DISTRICT

ATTACHMENT D

Non-Collusion Affidavit
(Form must be completed and returned with bid.)

Bibb County Board of Education, Macon GA 31208

I state that I am President & CEO (Title) of Securely Managed LLC (Name of Company)
And that I am authorized to make this affidavit on behalf of my firm, and its owners, directors, and officers. I am the person responsible in my firm for the price(s) and the amount of this bid and I state that this bid is made in good faith.

I state that:

1. The price(s) and amounts of this bid have been arrived at independently and without consultation, communication or agreement with any other contractor, bidder, or potential bidder; neither the approximate price(s) have been disclosed nor will they be disclosed before bid opening to any other contractor, bidder or potential bidder.

2. No attempt has been made or will be made to induce any firm or person to refrain from bidding on this contract, or to submit a bid higher than this bid, or to submit any intentionally high or noncompetitive bid or other form of complimentary bid.

Securely Managed LLC (Name of Company), its affiliates, subsidiaries, officers,
Directors and employees are not currently under investigation by any government agency and have not in the last three years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding on any public contract.

I understand and my firm understands that any misstatement in this affidavit is and shall be treated as fraudulent concealment from the Bibb County Board of Education of the true facts relating to submission of bids for this contract.

Sajay Rai - 08/18/2025 (Name/Date)

President & CEO (Title or Position)

Sajay Rai (Signature)

Offeror Affirmation Form

BIBB COUNTY SCHOOL DISTRICT

Attachment E
OFFEROR AFFIRMATION FORM:

Company Name: Securely Managed LLC
RFI Name: SEIM-SOC-XDR Solution
RFI Number: RFP-26-005

After careful examination of the solicitation document in its entirety, other documents and any addendum(s) issued, the undersigned proposes to satisfy all requirements in accordance with said documents.

For Consideration of this proposal, the undersigned hereby affirms that:

1. He/She is a duly authorized official of the offeror.
2. NO changes were made to the original RFI document,
3. The proposal is being submitted on behalf of the offeror in accordance with any terms and conditions set forth in this document.
4. The offeror will accept any awards made to it as a result of the proposal submitted here in for a minimum of one hundred and twenty (120) days following the date of submission.
5. The offeror will accept the terms and conditions set forth in the contract template attached here to.

If notified in writing by mail or delivery of the acceptance of the award, the undersigned agrees to furnish and deliver to the assigned procurement professional within five (5) days of the request, a certification of insurance indicating the coverage specified within this solicitation.

A contract shall be established which will set forth the terms of this agreement. The contract shall be interpreted, constructed, and give effect in all respects according to the laws of the State of Georgia.

Nondiscrimination in Employment: We, the supplier of goods, materials, equipment and services covered by this bid or contract, have not discriminated in the employment, in any way, against any person or person, or refused to continue the employment of any person or persons on account of their race, color, sex, religion, national origin, marital status, sexual orientation, age, or disability.

Respectfully Submitted,

Company Name Securely Managed LLC

Authorized Official Name Sajay Rai
Title: President & CEO

Signature Sajay Rai
Date: 08-18-2025

E-mail Address: sajayrai@securelymanaged.com

The legal name of the bidder is:
Securely Managed LLC

PLEASE PRINT OR TYPE RESPONSE

Certificate of Non-Collusion

BIBB COUNTY SCHOOL DISTRICT

Attachment F
CERTIFICATE OF NON-COLLUSION

By responding to this solicitation, the supplier understands and agrees to the following:
That the submitted response constitutes an offer, which when accepted in writing by the State Entity, and subject to the terms and conditions of such acceptance, will constitute a valid and binding contract between the undersigned and the State Entity; and
That the supplier has read the specifications and requirements shown or referenced in the solicitation and that the supplier's response is made in accordance with the provisions of such specifications and requirements except as expressly stated otherwise in the supplier's response; and
That the supplier guarantees and certifies that all items included in the supplier's response meet or exceed any and all such stated specifications and requirements of the solicitation except as expressly stated otherwise in the supplier's response; and
That, if awarded a contract, the supplier will deliver goods and/or services that meet or exceed the specifications and requirements of the solicitation except as expressly stated otherwise in the supplier's response; and
That the response submitted by the supplier shall be valid and held open for a period of **one hundred and twenty (120) days (or such other time period as identified in the solicitation)** from the final solicitation closing date and that the response may be held open for an additional period of time subject to the supplier's consent; and
That the supplier's response is made without prior understanding, agreement, or connection with any corporation, firm, or person submitting a response for the same materials, supplies, equipment, or services and is in all respects fair and without collusion or fraud. The supplier understands and agrees that collusive bidding is a violation of state and federal law and can result in fines, prison sentences, and civil damage awards; and
That the provisions of the Official Code of Georgia Annotated, Sections 45-10-20 et seq. have not been violated and will not be violated in any respect.

DO NOT MODIFY THE BID/PROPOSAL CERTIFICATION TERMS IN ANY WAY. THIS FORM MUST BE COMPLETED, SIGNED AND SUBMITTED WITH YOUR RESPONSE.

Contractor's Full Legal Name: (PLEASE TYPE OR PRINT)	Sajay Rai
Authorized Signature:	Sajay Rai
Printed Name and Title of Person Signing:	Sajay Rai - President & CEO
Date:	08-18-2025
Company Address:	131 Guilford Rd, Bloomfield Hills, MI 48304
FAX Number:	866-531-8620
Email Address:	sajayrai@securelymanaged.com
***This table must be completed in its entirety by the supplier.**	