

County of Lassen
ADMINISTRATIVE SERVICES

Memorandum

Date: December 5, 2024

Board Date: December 17, 2024

To: Board of Supervisors

From: Travis Stading, Technical Support Specialist II *TS*

Subject: Network Security Upgrade

Recommendation: Respectfully recommend that the Board: 1.) Approve the purchase from StepCG not to exceed \$950,000 and/or 2.) Authorize CAO to sign/execute purchase/agreement and/or 3.) provide direction to staff.

Background: The County's network is protected by a Firewall, Antivirus, and Virtual Private Network (VPN) solutions. The firewall solution we have is approaching its end-of-life and needs to be upgraded due to the growth of our network. The current Antivirus is a stand-alone system that does not provide visibility of traffic to the current firewall solution. The current VPN does not meet the County's needs for remote access to County resources.

Discussion: The request is to replace two primary firewalls, all antivirus, add managed security services, VPN for county resources, and vendor services for implementation. These purchases would also allow for ISD to remove approximately 10 pieces of aged equipment and increase network reliability to State resources. This would provide visibility of all traffic within the County network, providing better security and allow staff to quickly identify a cybersecurity incident. This purchase would cover the licensing and services for the next 5 years. This purchase would not be possible without the funding support of Community Social Services, and Health and Social Services. The product and services are listed under Omnia Contract 01-154.

Fiscal Impact: This purchase would be paid out of the Network Infrastructure fund (160-1601), Social Services Admin (120-0852), Protective Services (120-0853).

Alternatives:

1. Direct Staff to present other evaluated solutions at a later board meeting. (Other solutions evaluated did not meet the standards recommended by ISD.)
2. Do not purchase any security upgrade (Not recommended due to possible cyber security exposure.)



STEP CG, LLC
 50 E. Rivercenter Bldg, Suite 900
 Covington, KY 41011

Quote
 Quote Date: Mar 6, 2024
 Valid Till: Dec 27, 2024
 Quote Number : Q-28316

BILL TO:

Lassen County
 221 S. Roop St., Ste. 4
 Susanville, CA 96130

SHIP TO:

Lassen County
 221 S. Roop St., Ste. 4
 Susanville, CA 96130

Contact Name: Travis Stading

Quote Stage: Final

S.No.	Product Details	Qty	List Price	Discount	Total
1	Fortinet FG-3000F-BDL-809-60 :FORTIGATE-3000F HARDWARE PLUS 5 YEAR HARDWARE PLUS FORTICARE PREMIUM AND FORTIGUARD ENTERPRISE PROTECTION	2	\$ 490,890.75	\$ 441,801.68	\$ 539,979.82
2	Fortinet FC2-10-AZVMS-465-01-60 FortiAnalyzer-VM Subscription License with Support 5 Year Subscription license for 50 GB/Day Central Logging & Analytics. Include 24x7 FortiCare support, IOC, SOC subscription, and FortiGuard Outbreak Detection service.	1	\$ 44,275.00	\$ 19,596.12	\$ 24,678.88
3	Fortinet FC2-10-FEDR1-349-01-60 FortiEDR Discover, Protect & Respond and Standard MDR (100 seats MOQ) 5 Year FortiEDR Discover, Protect & Respond and Standard MDR Cloud Subscription and 24x7 FortiCare for 500 endpoints	1	\$ 225,000.00	\$ 72,000.00	\$ 153,000.00
4	Fortinet FC1-10-FEDR1-349-01-60 FortiEDR Discover, Protect & Respond and Standard MDR (100 seats MOQ) 5 Year FortiEDR Discover, Protect & Respond and Standard MDR Cloud Subscription and 24x7 FortiCare for 25 endpoints	3	\$ 14,375.00	\$ 14,369.25	\$ 28,755.75
5	Fortinet FC2-10-EMS05-485-01-60 Endpoint-based Licenses - Managed FortiClient 5 Year Managed FortiClient Subscription for 500 endpoints. Includes VPN/ZTNA Agent, EPP/APT, Deployment Assistance, Endpoint Monitoring Service and FortiClient Cloud with FortiCare Premium.	1	\$ 85,500.00	\$ 27,360.00	\$ 58,140.00
6	Fortinet FC1-10-EMS05-485-01-60 Endpoint-based Licenses - Managed FortiClient 5 Year Managed FortiClient Subscription for 25 endpoints. Includes VPN/ZTNA Agent, EPP/APT, Deployment Assistance, Endpoint Monitoring Service and FortiClient Cloud with FortiCare Premium.	3	\$ 7,880.00	\$ 7,564.80	\$ 16,075.20
7	Fortinet FC1-10-EDBPS-310-02-12 FortiCare BPS Subscription for FortiEDR 1 Year FortiEDR Best Practice Service for up to 999 Endpoints/users	1	\$ 6,500.00	\$ 1,950.00	\$ 4,550.00
8	Fortinet FC1-10-FCBPS-310-02-12 FortiCare BPS Subscription for FortiClient 1 Year FortiClient Best Practice Service for up to 999 Endpoints/users	1	\$ 3,000.00	\$ 900.00	\$ 2,100.00
				Sub Total	\$ 827,279.65
				Tax	\$ 39,148.54
				Grand Total	\$ 866,428.19

Terms and Conditions

NOTICE: Due to the ongoing supply chain shortage, your order may be delayed due to availability. All orders placed will normally ship when entire order is in-stock, instead of partial shipments as inventory becomes available. If you chose to allow partial shipments and invoicing, your order will ship and invoice as supply becomes available and may speed up the total order fulfillment. If you would like to have your order partially shipped, please notify your sales rep for an authorization form.

Shipping and state/local sales tax may apply.

STEP

STEP CG, LLC
50 E Rivercenter Blvd #900
Covington, KY 41011

QUOTE

Q-31852

Date Created Nov 26, 2024

Quote Stage Budgetary

Valid Until Dec 27, 2024

Sales Executive Nick Hughes

Contact Travis Stading

Bill To

Lassen County
221 S. Roop St., Ste. 4
Susanville, CA 96130

Ship To

Lassen County
221 S. Roop St., Ste. 4
Susanville, CA 96130

Line	Item & Description	Qty	Unit List Price	Discounted Unit Price	Extended Total
1	STEP CG Installation - 1 week on site - Remote design - Remote config - Remote trouble shooting - Remote consulting and advice - On call for firewall cutover - Knowledge transfer *Expected to be complete in 4-6 months*	1	\$ 60,000.00	\$ 60,000.00	\$ 60,000.00

Purchasing Contract: Fortinet Omnia Contract 01-154

Quote Total: \$ 60,000.00

Shipping and state/local sales tax may apply.

ORDER AUTHORIZED BY:

(Signed)

(Date)

(Print Name)



SERVICE DESCRIPTION

FORTIEDR™ & MDR SERVICES

1. Introduction

FortiEDR services are available to the end-user (the “Customer”) as two (2) lines of service:

- FortiEDR is a cloud-based software as a service, which provides an end-point protection platform, based on alerts communicated by collectors deployed in the Customer’s network (the “FortiEDR Service”). The FortiEDR Service delivers threat protection both pre- and post-infection in real time. The FortiEDR Service incorporates techniques to: prevent malware infection, detect and defuse security threats and to provide automated response and remediation with customisable playbooks.
- The FortiGuard™ Managed Detection and Response Services, requiring an active FortiEDR Service Bundle, add alert management with the aim to assure all customer alerts are acknowledged and addressed accordingly (the “MDR Service”). The MDR Service provides round the clock monitoring in order to provide protection for the Customer’s risk profile. For malicious alerts, Fortinet will actively contact the Customer to provide guidance to mitigate the threat.

2. Service Features and Deliverables

2.1 FortiEDR Service Bundles

The FortiEDR Service is delivered through the FortiEDR cloud platform which is managed by Fortinet on a twenty-four (24) hours a day by seven (7) days a week basis. FortiEDR cloud platform is monitored for server availability, service capacity, and network resource utilization and is based on the Google Cloud Platform for hosted services and computing infrastructure. Customers may choose the geographic region in which their FortiEDR platform components are located from the then-current available regions (currently, US Central, US East, US West, West Europe, East Europe, North America, South America, Asia East, Asia South, Asia Southeast, Asia Northeast and Australia).

The FortiEDR Service is offered bundled with the following security features:

- **Discover & Protect:** Pre-infection prevention engine based on Fortinet Next Generation Anti-Virus (NGAV) capabilities; post-infection real time protection; proactive risk mitigation that includes discovery of communicating applications and IoT devices, vulnerability management and application rating empowering attack surface reduction; orchestrated incident response that includes automated investigation and remediation capabilities. This service bundle is also referred to as Predict & Protect.
- **Protect & Response:** Pre-infection prevention engine based on Fortinet NGAV capabilities; post infection real-time protection; threat hunting capabilities with up to one (1) month data retention; forensics overview and control that includes attack graph with code tracing and orchestrated incident response that includes automated investigation and remediation capabilities. This service bundle is also referred to as Protect & Respond.
- **Discover, Protect and Response:** Pre-infection prevention engine based on Fortinet NGAV capabilities; post-infection real time protection; proactive risk mitigation that includes discovery of communicating applications and IoT devices, vulnerability management and application rating empowering attack surface reduction; threat hunting capabilities with up to one (1) month data retention; forensics overview and control that includes attack graph with code tracing and orchestrated incident response that includes automated investigation and remediation capabilities. This service bundle is also referred to as Predict, Protect & Respond.
- **XDR:** Add-on service bundle which provides data feed collection and signal correlation of data from multiple security products with the goal of increasing detection efficacy and improving security operations efficiency.

All FortiEDR Service bundles provide:

- Service availability target of 99.9%, with platform functionality available for 99.8% in any given calendar month.
- FortiCare™ 24x7 technical support, as outlined in the then-current Fortinet support policies and service description, available on the Support Portal or other site as designated by Fortinet.



2.2 FortiGuard™ Managed Detection and Response (MDR) Service

The MDR Service is delivered on a twenty-four (24) hours a day by seven (7) days a week basis. The MDR Service provides threat monitoring and hunting, analysis and response of security events in the Customer's FortiEDR environment, as reported to the console of either the FortiEDR Service or XDRservice add-on.

Contingent on the activation of the Service contract and completing the setup of the FortiEDR Service console through the Best Practice Service add-on, the Standard MDR or Managed XDR Service will enter a tuning period (the "Initial Tuning Period") which shall last for 6 weeks, during which events will be categorized to eliminate inconclusive or likely safe events allowing the Service beyond this stage to provide solely on malicious or suspicious activity. During this period the MDR team will make reasonable efforts to handle events based on the following targets:

Event Classification	Definition	Analyst Response Actions	Response Time During Initial Tuning Period (*Please note, this is not included in the Basic MDR Service*)
Malicious or Suspicious	Programs that are identified to have malicious capability, make changes to the system without user's consent, and have no commercially viable use.	Handled, customer notified if needed. Response can be configured to block immediately or take other actions as agreed upon with customer.	Standard MDR - Response action and notification within 1 hour. Follow-up within 24 hours.
			Managed XDR - Response action and notification within 1 hour. Follow-up within 24 hours.
Inconclusive	Programs producing activity initially determined to be suspicious and needs further investigation for verification if malicious or benign.	Handled, exception created, customer notified, and response action taken if determined to be malicious or new unwanted program based as agreed upon with customer.	Standard MDR - Event handled within 24 hours and a response action will take place and notification sent if deemed to be malicious within 1 hour.
			Managed XDR - Event handled within 24 hours and a response action will take place and notification sent if deemed to be malicious within 1 hour.
Confirmed Safe or Likely Safe	Legitimate software that was intended for use by Licensee (example: security software or business software)	Handled, exception created if needed	Standard MDR - Handled within 24 hours.
			Managed XDR - Handled within 24 hours.

For the remaining duration of the Service immediately following the Initial Tuning Period, a team of threat experts will, on behalf of the Customer, review and analyze malicious and suspicious security event generated in the FortiEDR and



or FortiXDR console, proactively hunt for threats, and take actions, as agreed with the Customer, to ensure they are protected according to their risk profile. The aim is to act upon events within a target time based on the generation of the event, in the FortiEDR console and according to the service level selected as follows:

Event Classification	Definition	Analyst Response Actions	Response Time
Malicious or Suspicious	Programs that are identified to have malicious capability, make changes to the system without user's consent, and have no commercially viable use.	Handled, either as genuinely malicious or as a false positive, customer notified if needed. Response can be configured to block immediately or take other actions as agreed upon with customer.	Basic MDR - Response action and notification within 1 hour. Follow-up within 48 hours.
			Standard MDR - Response action and notification within 1 hour. Follow-up within 24 hours.
			Managed XDR - Response action and notification within 1 hour. Follow-up within 24 hours.

The MDR service consists of three service levels including for each the following pro-active security elements:

2.2.1 Basic Managed Detection and Response (Basic MDR)

- *Review and analysis* of customer's malicious and suspicious events within forty-eight hours (48) of the event being reported to the FortiEDR console. The Service will provide a basic analysis of the event as communicated by Fortinet and shall exclude and proactive threat hunting.
- *Notification management.* Upon receiving an event in the FortiEDR console, the MDR team shall:
 - Validate all events with a classification of malicious or suspicious.
 - Investigate and report on previously known and unknown malware. For any malicious event, a notification will be sent to the Customer by email to describe the alert, the level of threat, and recommendations. If required, the Customer may request a conference call to obtain clarification on the analysis and any recommended remedial actions, which may involve assistance to the Customer in configuring a FortiEDR' playbook.
 - Perform incident response using the FortiEDR tool over the breadth of the customer's FortiEDR deployment. If the incident involves endpoints that do not have FortiEDR collectors installed, the incident will need to be referred to a full incident response service.
 - Escalation request tickets requests for support will be initiated as soon as the customer submits a ticket in FortiCare to the MDR queue and will be responded to within forty-eight (48) hours of receipt.
 - The MDR team will review all exceptions set in the Customer environment once per quarter, send reporting, and offer a follow-up call to discuss. The Customer is encouraged to request regular meetings at other intervals if needed, or ad-hoc, to review the findings of the exception review and discuss improvements to their security posture.

2.2.2 Standard Managed Detection and Response (Standard MDR)

This service level provides the following service features in addition to the deliverables of the Basic MDR Service:

- *Review and analysis of events* - will take place within twenty-four (24) hours of being reported to the FortiEDR console.
- *Notification management.* Upon receiving an event in the FortiEDR console, the MDR team shall:
 - Perform advanced investigation – if required, malicious artifacts may be obtained from collector endpoints for forensic analysis (e.g. Windows event log records, host files, scheduled log files, browser artifacts).
 - Perform tuning of the customer environment for the first 6 weeks after onboarding to the MDR service
- Escalation request tickets requests for support will be initiated as soon as the customer submits a ticket in FortiCare to the MDR queue and will be responded to within twenty-four (24) hours of receipt *Customized Onboarding* which requires the completion of a questionnaire to allow for customized handling of:



- Notification handling and response; and
- Information gathering for network, systems, applications and users.
- A review of MDR team specialized and customized security policy recommendations.
- Proactive Threat Hunting – custom queries run in the customer's FortiEDR threat hunting console tab in response to threat intelligence reports to identify potential threats and minimize risk
- Regular Meetings with the MDR Team – Customers must initiate the request to set up weekly, monthly, or quarterly meetings with the MDR team to discuss industry-specific threat intelligence, train their in-house SOC, or review best practices for exception setting in FortiEDR. The MDR team will review all exceptions set in the customer environment once per quarter, send reporting, and offer a follow-up call to discuss.

2.2.3 Managed XDR

For Customers who have purchased the XDR license as described in section 2.1, the following service features will be provided in addition to the Basic and Standard MDR Service entitlements:

- Review and analysis of events to additionally include analysis of information provided from the XDR service on non-FortiEDR security controls if available such as firewalls, email security appliances, network access control, and web application firewalls.

3. Scope and Conditions

3.1 Platform requirements

- The Customer acknowledges and accepts to comply with the system requirements to use the FortiEDR cloud platform. Fortinet may change the platform requirements from time-to-time and notify the customer in doing so via email. The Customer is solely responsible for choosing the appropriate level of the appropriate supported platform required by the FortiEDR Service to best suit their needs. The then-current supported platform requirements are available in the "Installation and Administration Guide" which is available on the website www.fortinet.com.

3.2 Customer Requirements

- Customer must use the FortiEDR Service or MDR Service for legitimate and lawful business purposes only. The FortiEDR Service and MDR Service are provided for the Customer internal business use and shall not be resold to third parties or used for managed services. The Customer is responsible for ensuring that its usage of the Service shall be in accordance with all applicable laws (including, but not limited, privacy and security laws) and proper controls and processes shall be implemented in this respect. Therefore, Fortinet explicitly advises the Customer to assess and ensure that the usage of the Service complies with local legislation prior to its any deployment.
- Should Fortinet discover any illegal activity, regardless of intent, the FortiEDR Service and MDR Service may be terminated without notice and where appropriate the relevant authorities notified.
- Correct technical issues and minimize the recurrence of technical issues, for which the Customer is responsible, that may prevent Fortinet from meeting the service levels or availability targets.
- Ensure that the XDR add-on service FortiAnalyzer™ data lake repository is deployed in the Customer environment on-site or in the cloud.
- All communication with the Fortinet assigned resources shall be conducted in a professional manner and in accordance with the services provided. The Customer is responsible to assign qualified personnel to facilitate the successful delivery of the Service.

3.3 Customer Exclusions

- In the event that continued provision of the Service to the Customer may compromise the integrity or security of the FortiEDR or Fortinet's systems, networks or reputation, the Customer agrees that Fortinet may permanently or temporarily limit or suspend these FortiEDR Service or MDR Service to the Customer at Fortinet's sole discretion.
- Accept that Fortinet is not responsible for any loss of connectivity by the Customer, where the FortiEDR or MDR Service will considered as being utilized.



3.4 MDR Service requirements

- For first time usage, the pre-requirements for the MDR Service are: (a) purchase and completion of the FortiEDR Deployment Service; and (b) end-point collectors covered by the Service shall be configured into prevention mode to actively monitor threats.
- Customer will provide in a timely fashion all information, support, approvals and resources needed by Fortinet team to successfully deliver the MDR Service:
 - Provide relevant application knowledge associated with an alert or a request.
 - Provide any other data that Fortinet may reasonably request in order to reproduce operating conditions similar to those present when the relevant alerts or issues occurred.
 - Carefully monitor emails from Fortinet on an on-going basis as a requirement for the delivery of the MDR Service.
 - To remediate vulnerabilities on protected systems within fourteen (14) days of any threat notification by Fortinet. The Customer agrees that Fortinet's response time targets as documented in Section 2.2 do not apply to protected systems that are pending remediation for more than fourteen (14) days after initial notification by Fortinet.
- Customer shall provide and maintain with Fortinet a list of up to three (3) designated contacts. No more than one (1) change a quarter may take place to this list. These are the only contacts authorized on the Customer's behalf to make and respond to inquiries regarding alert management services to Fortinet.
- All contact by the Customer with the Service shall be through a ticket raised in the customer support portal at <https://support.fortinet.com> and explicitly excludes any email sent to Fortinet by the Customer irrespective of the sender being identified as a designated contact.
- XDR Service requires the prior activation and appropriate configuration of XDR to ensure the relevant data is available in the FortiEDR console.
- If requested, the delivery of the Quarterly Briefing via a web conference will take place using Fortinet resource during the core business hours of 09:00 to 18:00 in the time zone local where the work is being delivered.

3.5 General Conditions and Disclaimers

- There are regularly scheduled maintenance of the Fortinet infrastructure which takes place on the first and third Sunday of each month between 02.00 and 11.00 (EST). During the maintenance, Fortinet will make efforts to perform such maintenance without any service disruption. It may occur during these maintenance windows that the FortiEDR central manager is unavailable for up to thirty (30) minutes. During this time, data collection will not be disrupted, and end-points will remain protected.
- In the event that the integrity of the Service is at risk, Fortinet may perform emergency maintenance actions at their sole discretion. Fortinet will make efforts to inform all affected parties within one (1) hour of the start of the maintenance activity.
- The Customer acknowledges and agrees that: (a) FortiEDR Service and MDR Service are subject to intrinsic reliability and technical limitations; (b) FortiEDR Service and MDR Service help to prevent, find or eliminate malware and security breaches but it is technically impossible to guarantee email or network security as no security device or service can guarantee full security or the blocking of all known malicious activity; and (c) Fortinet accepts no liability for any damage or loss resulting directly or indirectly from any failure of FortiEDR Service and MDR Service to detect malware, malicious activity or for false positives including security breach, data loss, data corruption, and service interruptions and/or degradations of the Company's network, systems.
- Unless otherwise specified, the FortiEDR and MDR Service will be delivered in English and remotely.
- The Customer understands that the FortiEDR Service and the MDR Service are designed to supplement and support, but not to replace, the implementation of an effective end-user computer usage policy by the Customer across its organization.
- The scope of the service is limited to the FortiEDR and MDR Service as outlined in this document. Any request by the Customer for services beyond the duration or scope will be provided at Fortinet's discretion and billable at the then-current rate.
- All MDR Service levels described in this document are targets which Fortinet will make efforts to achieve and are measured on receipt of an alert in the FortiEDR console.



- By purchasing the FortiEDR or MDR Service, Customer understands and agrees that Fortinet is not obligated to provide the service if Customer fails to meet the requirements under section 3.
- Fortinet will retain the configuration and any associated data only for a period of fourteen (14) days to allow data collection or service re-initiation following termination or expiration of the Service or the end of agreed Service's evaluation period. Once such period is elapsed, the Customer instance will be deleted along with any associated data.
- Customer represents and warrants that it has all rights, permissions, and consents necessary to: (a) submit personal data to deliver the FortiEDR Service, MDR Service, and necessary support; and (b) grant Fortinet the right to process personal data for the provision of the FortiEDR Service, MDR Service, and support: (i) as required by applicable law; (ii) as reasonably requested by the Customer; (iii) as necessary to provide the FortiEDR Service, MDR Service, and related support, and prevent or address technical problems or violations of the FortiEDR Service, MDR Service; and (iv) as set forth in the following sentence. Fortinet will process the personal data that Fortinet receives through the Service pursuant to: (a) a data processing agreement executed between the parties where required under applicable law, and (b) the provisions of the Fortinet Privacy Policy located at <http://www.fortinet.com/aboutus/privacy.html> ("Privacy Policy"), updated from time to time at Fortinet's discretion. When the FortiEDR Service or MDR Service provides Customer with new personal data that Customer did not already possess (such as the Service's determination that a particular email poses a security threat), Customer may use this new personal data solely for Customer's lawful internal cybersecurity purposes.
- The FortiEDR and MDR Service are subject to the terms of Fortinet's Service Terms & Conditions located at <https://www.fortinet.com/corporate/about-us/legal.html>.

3.6 Service Availability Levels

The service availability levels described in this document are targets which Fortinet will make efforts to achieve and will exclude delays related to Service unavailability or disruption caused by any of following events, without limitation:

- scheduled maintenance or emergency maintenance;
- Customer's -initiated changes whether implemented by Customer or Fortinet or a third party on behalf of Customer;
- Customer's failure to adhere to Fortinet implementation, support processes and procedures;
- acts or omissions of the Customer, its employees, agents, third party contractors or vendors or any third party accessing the Service;
- any violations of the Customer or Scope & Conditions defined above;
- any event not wholly within the control of Fortinet;
- negligence or willful misconduct of the Customer, or others authorized by the Customer to use the Services provided by Fortinet;
- any failure of any component for which Fortinet is not responsible, including but not limited to all Customer infrastructure including electrical power sources, networking equipment, computer hardware, computer software or email content;
- any failures that cannot be corrected because the Customer, its systems or networks are not reasonably accessible to Fortinet. It is the Customer's responsibility to ensure that contact details are kept up to date and to confirm or update the existing the technical contact details.

4. Eligibility & Purchasing

The FortiEDR Service and MDR Service are available for purchase by a Customer through authorized Fortinet resellers and distributors globally. Fortinet authorized distributors are independent third parties that conduct business in their own name and account and, consequently, cannot bind Fortinet in any way. The FortiEDR Service and MDR Service are delivered to the Customer as referenced in the purchase order placed with Fortinet by the authorized distributor. The duration of the FortiEDR Service and MDR service are three hundred and sixty-five (365) days from service unit activation in accordance with Fortinet's registration policies. All sales are final.

The FortiEDR Service is available for purchase with a minimum of five hundred (500) end-point collectors with increments of twenty-five (25), five hundred (500), two thousand (2,000) or ten thousand (10,000) end-point collectors.




The XDR Service is available for purchase only for "Protect and Respond" or "Predict Protect and Respond" FortiEDR Service bundle.

The MDR Services are available as add-ons per the different FortiEDR Service bundles as per the following table

	Discover & Protect	Protect & Respond	Discover, Protect & Respond
Basic MDR	Add-on	Add-On	Add-On
Standard MDR		Add-On	Add-On
Managed xDR*		Add-On	Add-On

* XDR add-on pre-requisite

Approved as to Form

 JUN 18 2024

Lassen County Counsel



NCPA An Omnia Partners Company
Fortinet Contract 01-154 Authorized Reseller Partners

Reseller Name	Contact	Email
11:11 Systems	Matthew Parsons	matthew.parsons@1111systems.com
43tc	Matt McDermott	matt@43tc.com
5S Technologies	Michael Overton	michael.overton@5stechnologies.com
ACC Technical Services, Inc (Acctek)	Paul White	pwhite@acctek.com
Ahead, Inc.	Brooks Souders	brooks.souders@ahead.com
Airgap Labs LLC	Frank Wang	fwang@airgaplabs.com
All Covered	Michael Parezo	mparezo@allcovered.com
AMS.NET	Thomas Vasconi	tvvasconi@ams.net
Aquila, Inc.	Aaron Jaramillo	aaronj@aquilagroup.com
Aspire Technology Partners, LLC	Daniel Bongiovanni	teamaspire@aspiretransforms.com
BCI, Inc.	Robin Carpenter	rcarpenter@bcianswers.com
Blackhawk Data	Maryanne Pagano	mpagano@blackhawk11.com
BorderLAN Security	Diane Rogers	diane@borderlan.com ; deena@borderlan.com
C2 Enterprises	Phil Thompson	philip.thompson@c2itsystems.com
Carolina Advanced Digital	Susan Jabbusch	susan@cadinc.com
Carousel Industries of North America, LLC	Lauren Testa	ltesta@carouselindustries.com
Chromis Technology, LLC	Zach Garcia	zgarcia@chromis.com
CNI Sales, Inc.	Tim Kirk	timkirk@cnisalesinc.com
Compuquip Cybersecurity	Luis Santiago	lsantiago@compuquip.com
Computacenter	Mitzi Justice	mitzi.justice@computacenter.com
CCNY Tech	Jason Germond	jason.germond@ccnytech.com
ComSource	Phil Gadsden	pgadsden@comsourceny.com
Continental Resources, Inc. (ConRes)	Lou Novakis	lnovakis@conres.com
Converge Technology Solutions	Lynda Thomas	ContractSalesSupport-PublicSector@convergetp.com
C Spire Business (TekLinks dba C Spire Business)	Hollye Massey	hmassey@cspire.com
DataFree'd	Mike Phalovich	mpahalovich@datafreed.com
Delta Network Services LLC	Michael McGregor	mike.mcgregor@delta-ns.com
DGR Systems	Amanda Dugger	adugger@dgrsystems.com
DOF Creations, LLC.	Saeed Gordon	sbgordon@dofcreations.com
Dox Electronics	Ken Schwartz	kens@doxnet.com
DyntekServices dba Arctiq	Darlene Pricher	darlene.pricher@dyntek.com
EduTek Ltd	Mario Caligiuri	mario.caligiuri@edutekltd.com
ePlus Technology, Inc.	Amy Knower	Amy.Knower@eplus.com
ESX Technology Solutions	Renee Ramirez	rramirez@esxtech.com
General Datatech (GDT)	Jennifer Childs	jennifer.childs@gdt.com
GLS, Inc.	Joey Fields	jfields@gls.com
Gulf South Technology Solutions, Inc	James Moak	james@gulfsouthtech.com
GST	Phillip Lin	phillipl@gstinc.com
Heartland Business Solutions	Partner Relations	inquiry@hbs.net
Hypertec USA	Mike Marracino	mmarracino@hypertec.com
iConvergence	Beau Peyton	beaup@iconvergence.com
Infobond	Jo Davalos	wyragui@infobond.com ; jdavalos@infobond.com
In-Telecom Consulting LLC	Shawn Torres	storres@in-telecom.com
InterDev LLC	Gary Nichols	GNichols@Interdev.com
ISG Technology	Michael Reece	mreece@isgtech.com
ISSQUARED, Inc.	Lee Craft-Gobeille	curt.hedges@ncanet.com ; lee.craft@ncanet.com
Katalyst	Luke Johnson	ljohnson@katalystng.com
Layer 3 Communications	Paula Sands	psands@layer3com.com
Layer8 Consulting	Elden Quesinberry	equesinberry@L8C.com
Liquid Networkx	Robert Short	Ateam@liquidnetworkx.com
Mission Critical Systems	Maryanne Caruso	mcaruso@locked.com
MXN Corporation	Deborah Arnett	insidesales@mxncorp.com
Nth Generation Computing Inc	Steve Jung	Steve.Jung@nth.com
NetSync	Jeff Barker	jbarker@netsync.com
Network Experts of New York	Anu McGowan	anu@albany-technology.com
PC Solutions & Integration	David Rudnick	david@pcsusa.net
Peak Methods	Jennifer McCuistian	peak.accounting@peakuptime.com ; Jennifer.McCuistian@peakuptime.com
PIER Group LLC	Chad Williams	cwilliams@piergroup.com
PNG Telecommunications Inc., dba Powernet	Tony Wells	twells@powernetco.com
PNW Security LLC	Derek Hanson	derek@pnwsecurity.com

PremCom Corporation	Joe Griffo	jgriffo@premcom.com
Presidio	Jackie Arnett	jarnett@presidio.com
Prosys	Mitzi Justice	mitzi.justice@prosys.com
Right! Systems Inc. (RSI)	Sean Padget	SPadget@rightsys.com
Optimus TechServices, LLC DBA Seamless Advan	Steven Frank	sfrank@sas-us.com
Scientel Solutions	Glenn Luckman	gluckman@scientelsolutions.com
SHI	Hannah Visbeen	PS_Contracts@shi.com
Sun Management	John Samuel	jsamuel@sunmanagement.net
Structured Communication Services, Inc.	Casey Richmond	crichmond@structured.com
Step CG	Luke Gurekovich	lgurekovich@stepcg.com
Surelock Technology	Guy Anderson	ganderson@surelocktechnology.com
Terawolf Technologies Inc	Gaylord Van Brocklin	gvb@terawolf.com
Universal Data	Stephanie Kavanaugh	skavanaugh@udi.com
United Data Technologies	Mike Hendrix	mhendrix@udtonline.com
Verinext	Drew Campbell	drew.campbell@verinext.com
Vector Resources, Inc. dba VectorUSA	Briana Borrenpohl	bfernandes@vectorusa.com
World Wide Technologies	Matt Lang	Matthew.Lang@wwt.com ; Carol.Harting@wwt.com
Xigent Solutions	Barb Canham	barbcanham@xigentsolutions.com
Xiologix LLC	Sheryl Still	inside_sales@xiologix.com
Xtel Communications	Harbinder Goraya	harbinder@xtel.net
Yellow Dog Networks	Chris D'Amore	cdamore@yellowdognetworks.com
Zivaro	Sean McCroskey	smccroskey@zivaro.com