

FAX COVER SHEET

TO	Buyer: Jessica S. Chambers
COMPANY	State of West Virginia
FAX NUMBER	13045583970
FROM	Esteve Mede
DATE	2019-07-30 17:06:15 GMT
RE	EEC Response to - CRFQ-0210-ISC2000000002-2

COVER MESSAGE

Hello Ms. Chambers,

EEC is Service Disabled Veteran-Owned Small Business and SBA 8a Certified. We are very please to submit our response to the about RFQ. We are offering the best tool in the market for this opportunity. We are looking forward to working with you soon.

Thank you,

Esteve Mede

emedede@eecomputing.com

RECEIVED
 2019 JUL 30 PM 1:08
 WV PURCHASING
 DIVISION

FAX COVER SHEET

TO	Buyer: Jessica S. Chambers
COMPANY	State of West Virginia
FAX NUMBER	13045583970
FROM	Esteve Mede
DATE	2019-07-30 17:06:15 GMT
RE	EEC Response to - CRFQ-0210-ISC2000000002-2

COVER MESSAGE

Hello Ms. Chambers,

EEC is Service Disabled Veteran-Owned Small Business and SBA 8a Certified. We are very please to submit our response to the about RFQ. We are offering the best tool in the market for this opportunity. We are looking forward to working with you soon.

Thank you,

Esteve Mede

emedede@eecomputing.com

RECEIVED
 2019 JUL 30 PM 1:10
 WV PURCHASING
 DIVISION

FAX COVER SHEET

TO	Buyer: Jessica S. Chambers
COMPANY	State of West Virginia
FAX NUMBER	13045583970
FROM	Esteve Mede
DATE	2019-07-30 17:06:15 GMT
RE	EEC Response to - CRFQ-0210-ISC2000000002-2

COVER MESSAGE

Hello Ms. Chambers,

EEC is Service Disabled Veteran-Owned Small Business and SBA 8a Certified. We are very please to submit our response to the about RFQ. We are offering the best tool in the market for this opportunity. We are looking forward to working with you soon.

Thank you,

Esteve Mede

emedede@eecomputing.com

RECEIVED
 2019 JUL 30 PM 1:18
 WV PURCHASING
 DIVISION

EXHIBIT A – Pricing Page
EndPoint Detection and Response Services - OT19125
Note to Vendors: The Pricing Page is locked with the exception of Unit Cost column.

Line Items	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1	Contract Item: Endpoint Detection and Response Software for approximately 2,000 EndPoints	LS	1	\$18,500.00	\$ 18,500.00
4.1	Optional Renewal Year 2 Maintenance: Contract Item: Endpoint Detection and Response Software	LS	1	\$18,500.00	\$ 18,500.00
4.1	Optional Renewal Year 3 Maintenance: Contract Item: Endpoint Detection and Response Software	LS	1	\$18,500.00	\$ 18,500.00
4.1	Optional Renewal Year 4 Maintenance: Contract Item: Endpoint Detection and Response Software	LS	1	\$18,500.00	\$ 18,500.00
Total Overall Cost					\$ 74,000.00

Line Items	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
------------	-------------	-----------------	--------------------	-----------	---------------

Please note: This information is being captured for auditing purposes

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 WV Purchasing Division as Change Orders for subsequent years.



7/302019

Vendor Signature:

End to End Computing

SDVO * CYBER SECURITY * PROJECT MANAGEMENT * BIG DATA

CRFQ,0210,ISC2000000002

Request for Quotes (RFQ)

EndPoint Detection and Response Software

From

End-to-End Computing, LLC
2317 Jefferson Davis Hwy, 102
Alexandria, VA 22301
Phone: 571-449-6554
Fax: 571-732-3128
emedede@eecomputing.com
www.eecomputing.com

To

Department of Administration Office of Technology

POC: Jessica S Chambers

Duns #: 078442180

Taxpayer Identification Number (TIN): 45-4989462

CAGE #: 6Q9Y9

Service Disable Veteran-Owned Small Business (SDVOSB)

Response due Date & Time: July 30,2019 1:00 pm EST

End to End Computing

DEVELOP • CYBERSECURITY • PROJECT MANAGEMENT • BIG DATA



SentinelOne™

SentinelOne Core has all endpoint security essential features in place, including prevention, detection, and response in a single, purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

Key Features

- Single, holistic agent for PC, Mac, Linux, VDI
- Multi-layered AI-powered endpoint protection
- Threat Hunting and device controls
- Policy driven response to threats

Key Benefits

- Enterprise proven and easily scalable
- Certified and recognized as an industry leading solution
- Helps eliminate notification fatigue

The innovative security solution offers broad protection against diverse modes of attack, including:

Malware

- Executables - Trojans, malware, worms, backdoors, payload-based
- Fileless - Memory-only malware, no-disk-based indicators

Exploits

- Documents - Exploits rooted in Office documents, Adobe files, macros, spear phishing emails
- Browser - Drive-by downloads, Flash, Java, Javascript, VBS, IFrame/HTML5, plug-ins

Live/Insider

- Scripts - Powershell, WMI, PowerSploit, VBS
- Credentials - Mimikatz, credentials scraping, tokens

End to End Computing

PHONE * CYBERSECURITY * PROJECT MANAGEMENT * BIG DATA

SentinelOne Core delivers multi-layered AI-powered endpoint protection, with Static AI pre-execution protection for known and unknown file based malware, and Behavioral AI agent-side behavioral monitoring that covers any attack vector, including unknown exploits and bypass attempts of traditional anti-virus.

The Behavioral AI engine is built to detect and mitigate malicious code and scripts in documents and is capable of detecting fileless attacks and exploits. Lateral Movement uses Behavioral AI to discover attempts coming from another device over the network.

SentinelOne Core offers attack remediation, cleaning all artifacts of a malicious attempt, including registry, scheduled tasks and more, while Rollback Revert returns an endpoint its pre-infected state. Upon detection, SentinelOne can immediately stop lateral threat spread cold by disconnecting the infected endpoint from the network while still maintaining the agent's connection to the management console.

SentinelOne Core includes basic EDR/Threat Hunting, which provides the ability to search for attack indicators, investigate existing incidents, perform file integrity monitoring and root out hidden threats. It includes an Attack Storyline, a visual diagram representing an execution flow, helping IR teams to quickly evaluate the impact of any threat.

In addition, Device Control enables you to apply policy and control USB and peripheral devices connected to your assets.