March 13, 2024

EDMONDS COLLEGE, contemplates awarding a sole source contract to Oxygen Forensics Inc to provide software and hardware for forensic analysis of Unmanned Aerial Vehicles (UAVs – aka drones) and handheld computing devices, to include mobile phones, tablets, and devices with Global Positioning System (GPS) capability.

EDMONDS COLLEGE requires peer reviewed, tested, and industry accepted hardware and software to conduct forensic examinations so that students are exposed to the same tools in the classroom as what they'll be using in the industry, be it for law enforcement, corporate investigation, or private digital forensic analysis.

EDMONDS COLLEGE will enter into a THREE YEAR contract with Oxygen Forensics Inc. The contract will be issued on or after April 8, 2024 and will continue for a THREE year initial term. The cost of this THREE year contract is $68,121.86.

Offerors contemplating the above requirements are required to submit capability statements detailing their ability to meet the state's requirements within five (5) working days of this announcement.

Capability statements should address the following state requirements:

The capability to bypass personal identification number (PIN) and pattern locked devices, as well as the functionality to extract, document, and display:

• Device information – Phone Number, IMEI, IMSI, MEID, ESN & MAC ID
• Phonebook – contact names and numbers
• Text and picture messages
• Videos and pictures to include geotag location information and creation date and time stamps
• Emails and web browsing information
• GPS and location information including: date, time, longitude, latitude, and elevation in meters
• Social networking messages and contacts
• Deleted data – call logs, messages, emails
• Attached media or memory card contents (Pictures, Files, app data – located on media card)
• Wireless (Wi-Fi) networks used by the device

Additional requirements include the ability to:

• Gain access to popular cloud services like WhatsApp, Telegram, iCloud, Google, Samsung, Microsoft, Facebook, Instagram, and Twitter
• Extract data from over 31,000 devices
• Extract and analyze drone data from physical dumps, drone logs, and mobile applications
• Extract and analyze data from the most popular IoT devices: Amazon, Alexa, and Google Home
• Extract and analyze data from Windows, Linux, and macOS.
• Extract from the most popular health apps: Apple Health, Samsung Health, Huawei Health, and Fitbit
• Import numerous backups and images, including iTunes, Android, GrayKey, JTAG, Chip-off, UFED, XRY images, .dar archives, and Warrant Returns.

In the absence of other qualified sources, it is the state's intent to make a sole source award the contract.

To submit capability statements or for questions, contact:

Name: Kelvin Nesvog
Phone: 425.640.1586
Email: kelvin.nesvog@edmonds.edu