February 5, 2024

Arqit and Carahsoft Partner to Bring Symmetric Key Agreement Cybersecurity Product to the US Public Sector

Groundbreaking Cybersecurity Solution Now Available to US Government Agencies

LONDON and RESTON, Va., Feb. 05, 2024 (GLOBE NEWSWIRE) -- Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) (Arqit), a leader in quantum-safe encryption, and Carahsoft Technology Corp., The Trusted Government IT Solutions Provider®, today announced a partnership. Under the agreement, Carahsoft will be Arqit's Master Government Aggregator®, making Arqit's unique Symmetric Key Agreement Platform available through Carahsoft's reseller partners and NASA Solutions for Enterprise-Wide Procurement (SEWP) V, Information Technology Enterprise Solutions – Software 2 (ITES-SW2), National Association of State Procurement Officials (NASPO) ValuePoint, E&I Cooperative Services Contract and OMNIA Partners contracts.

Cyber adversaries employing "store-now, decrypt-later" attacks and stockpiling encrypted data to crack it open with quantum computers, presents long-term danger to organizations with sensitive data. Arqit's Symmetric Key Agreement Platform will enable end-customers to move simply and securely from a complex public-key infrastructure, which is vulnerable to a powerful quantum computer and relies on third parties, to a platform that is designed for the cloud and a world of connected devices.

"We are pleased to partner with Carahsoft to enable organizations to benefit from our unique Symmetric Key Agreement Platform, which hardens existing networks up to quantum-safe levels," said **David Williams, Arqit Founder, Chairman and CEO**. "Using our groundbreaking product, end-customers can simplify and strengthen their encryption to keep their data safe from current and future cyber threats."

"With the addition of Arqit's Symmetric Key Agreement Platform to our offerings, we are able to provide government agencies with the cutting-edge cybersecurity products required to meet newly enhanced regulations," said **Brian O'Donnell, Vice President of Cybersecurity Solutions at Carahsoft**. "We look forward to working with Arqit and our reseller partners to supply the Public Sector with advanced cryptographic technology that will ensure the resilience of our critical systems."

Arqit's solutions are available through Carahsoft's SEWP V contracts NNG15SC03B and NNG15SC27B, ITES-SW2 Contract W52P1J-20-D-0042, NASPO ValuePoint Master Agreement #AR2472, E&I Contract #EI00063~2021MA and OMNIA Partners Contract #R191902. For more information, contact the Carahsoft team at (571) 662-4771 or EcosystemVendors@carahsoft.com.

About Arqit

Arqit Quantum Inc. (Nasdaq: ARQQ, ARQQW) (Arqit) supplies a unique encryption Platform as a Service which makes the communications links of any networked device, cloud machine or data at rest secure against both current and future forms of attack on encryption – even from a quantum computer. Compliant with NSA standards, Arqit's Symmetric Key Agreement Platform delivers a lightweight software agent that allows devices to create encryption keys locally in partnership with any number of other devices. The keys are computationally secure and operate over zero trust networks. It can create limitless volumes of keys with any group size and refresh rate and can regulate the secure entrance and exit of a device in a group. The agent is lightweight and will thus run on the smallest of end point devices. The Product sits within a growing portfolio of granted patents. It also works in a standards compliant manner which does not oblige customers to make a disruptive rip and replace of their technology. Recognised for groundbreaking innovation at the Institution of Engineering and Technology awards in 2023, Arqit has also won the Innovation in Cyber Award at the National Cyber Awards and Cyber Security Software Company of the Year Award at the Cyber Security Awards. Arqit is ISO 27001 Standard certified. www.arqit.uk

About Carahsoft's Cybersecurity Solutions Portfolio

Carahsoft's Cybersecurity solutions portfolio includes leading and emerging technology vendors that enable organizations to defend against cyber threats, manage risk and achieve compliance. Supported by dedicated Cybersecurity product specialists and an extensive ecosystem of resellers, integrators and service providers, we help organizations identify the right technology for unique environments and provide access to technology solutions through our broad portfolio of contract vehicles. Our cybersecurity portfolio includes solutions for Supply Chain Risk Management, Cloud Security, Network & Infrastructure, Identity & Access Management, Risk & Compliance and more, ensuring comprehensive protection for organizations' cyber ecosystems. Explore Carahsoft's Cybersecurity solutions further here.

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®, supporting Public Sector organizations across Federal, State and Local Government agencies and Education and Healthcare markets. As the Master Government Aggregator® for our vendor partners, we deliver solutions for Cybersecurity, MultiCloud, DevSecOps, Big Data, Artificial Intelligence, Open Source, Customer Experience and Engagement and more. Working with resellers, systems integrators and consultants, our sales and marketing teams provide industry leading IT products, services and training through hundreds of contract vehicles. Visit us at www.carahsoft.com.

Media relations enquiries:

Arqit: pr@arqit.uk
Gateway: arqit@gateway-grp.com

Mary Lange
(703) 230-7434
pr@carahsoft.com

Investor relations enquiries:

Arqit: investorrelations@arqit.uk
Gateway: arqit@gateway-grp.com

Notes to Editors

"Store-now, decrypt-later" is a known threat and concerning for data with a long-time value:

- **US Congress:** "The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers and wait until sufficiently powerful quantum systems are available to decrypt it" (Congress, Quantum Computing Cybersecurity Preparedness Act, 21 December 2022, link).

Symmetric cryptography is a solution that can be implemented right now and can be used for both encryption and key exchange:

- **US National Security Agency (NSA):** "NSA considers using pre-shared symmetric keys in a standards-compliant fashion a better near-term post-quantum solution than implementing experimental post-quantum asymmetric algorithms" (NSA, The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, 7 September 2022, link).

The US Government has already directed their agencies to implement symmetric-key protections for National Security Systems (NSS):

- **The White House:** "By December 31, 2023, agencies maintaining NSS shall implement symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges" (The White House, National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 4 May 2022, link).

Caution About Forward-Looking Statements
This communication includes forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements, other than statements of historical facts, may be forward-looking statements. These forward-looking statements are based on Arqit's expectations and beliefs concerning future events and involve risks and uncertainties that may cause actual results to differ materially from current expectations. These factors are difficult to predict accurately and may be beyond Arqit's control. Forward-looking statements in this communication or elsewhere speak only as of the date made. New uncertainties and risks arise from time to time, and it is impossible for Arqit to predict these events or how they may affect it. Except as required by law, Arqit does not have any duty to, and does not intend to, update or revise the forward-looking statements in this communication or elsewhere after the date this communication is issued. In light of these risks and uncertainties, investors should keep in mind that results, events or developments discussed in any forward-looking statement made in this communication may not occur. Uncertainties and risk factors that could affect Arqit's future performance and cause results to differ from the forward-looking statements in this release include, but are not limited to: (i) the outcome of any legal proceedings that may be instituted against the Arqit, (ii) the ability to maintain the listing of Arqit's securities on a national securities exchange, (iii) changes in the competitive and

regulated industries in which Arqit operates, variations in operating performance across competitors and changes in laws and regulations affecting Arqit's business, (iv) the ability to implement business plans, forecasts, and other expectations, and identify and realise additional opportunities, (v) the potential inability of Arqit to successfully deliver its operational technology, (vi) the risk of interruption or failure of Arqit's information technology and communications system, (vii) the enforceability of Arqit's intellectual property, and (viii) other risks and uncertainties set forth in the sections entitled "Risk Factors" and "Cautionary Note Regarding Forward-Looking Statements" in Arqit's annual report on Form 20-F (the "Form 20-F"), filed with the U.S. Securities and Exchange Commission (the "SEC") on 21 November 2023 and in subsequent filings with the SEC. While the list of factors discussed above and in the Form 20-F and other SEC filings are considered representative, no such list should be considered to be a complete statement of all potential risks and uncertainties. Unlisted factors may present significant additional obstacles to the realisation of forward-looking statements.

Source: Arqit