Sekur Private Data Adds Q Branch Red Team to Scale and Harden Its Platform for C-Suite, Government and Defense Growth

Q Branch brings Fortune 500, federal, and military cybersecurity experience; team will be responsible for Sekur's security, code monitoring and improvements, and new feature roll-out and quality control as the Company prepares for planned C-suite, government, and defense account additions and international expansion.

MIAMI, FL — November 24, 2026 — Sekur Private Data, Inc., a Miami-based Swiss-hosted cybersecurity, private communications, and defense communications company serving enterprise, government, and defense clients, and a wholly owned U.S. subsidiary of Sekur Private Data (OTCQB: SWISF | CSE: SKUR | FRA: GDT0) ("Sekur" or the "Company"), today announced that it has added **Q Branch, Sekur's Post-Quantum Security Branch**, a dedicated Red Team cybersecurity and technology leadership team, to its technology organization. Q Branch has been brought in to help Sekur **scale its platform, tighten security, and maintain highly secure systems**, and is ready to scale with the Company's **planned addition of new C-suite, government, and defense accounts, including its expansion into government and defense markets internationally**. Q Branch will be responsible for Sekur's security, code monitoring and improvements, and new feature roll-out and quality control. In consideration for Q Branch's services, Sekur's publicly traded parent company, Sekur Private Data Ltd., has issued **6,000,000 common shares of Sekur Private Data Ltd. for services already rendered** and granted **2,000,000 stock options of Sekur Private Data Ltd. exercisable at US$0.10 per option for a period of two years**, for services to be rendered through December 31, 2028.

A Red Team approaches an organization's systems the way a capable adversary would: it continuously probes the code, infrastructure, and operational procedures for weaknesses so they can be found and fixed before they can be exploited. For Sekur, whose clients include **defense and federal officials, government agencies, military commands, enterprises, and executives handling Controlled Unclassified Information (CUI)**, Q Branch adds an offensive-security discipline alongside ongoing engineering, so that security keeps pace with new features and a growing user base.

"Our clients trust us with communications that adversaries actively want to intercept, and the only responsible way to protect them is to attack our own systems before anyone else does," said Alain Ghiai, Founder and CEO of Sekur Private Data. "**Adding Q Branch gives us the capacity to tighten security across the entire platform while we continue to improve the code and ship new features.** It is a core part of how we prepare to scale."

"We are planning for significant account growth among C-suite executives, governments, and defense organizations, including expansion into government and defense markets internationally, and those clients hold us to the highest standard. **Q Branch is ready to scale with us**, so that every new account and every new government deployment is supported by systems that are tested, hardened, and maintained to that standard."

Q Branch's Mandate

Q Branch's services will focus on three areas, in order of priority: first, **security**, including adversarial testing of Sekur's applications, infrastructure, and Swiss-hosted and on-premises deployment models, and remediation of any weaknesses identified; second, **code monitoring and improvements**, including the proprietary HeliX data transfer architecture that underpins SekurOne and SekurVPN; and third, **new feature roll-out and quality control** across SekurOne, SekurMail, SekurMessenger, SekurVPN, and SekurRelay.

Q Branch has already tested Sekur's platform against **AI-driven intrusion techniques**, in which attackers use artificial intelligence to automate reconnaissance, discover vulnerabilities, and launch attacks at a speed and scale beyond traditional methods. **Q Branch will maintain a high level of vigilance to protect Sekur against such attacks**, continuing to test the platform against evolving AI-enabled threats as part of its ongoing mandate.

About Q Branch: Sekur's Post-Quantum Security Branch

Q Branch, Sekur's Post-Quantum Security Branch, is the Company's cybersecurity and technology leadership team. It brings decades of combined cybersecurity experience supporting **Fortune 500 enterprises, federal agencies, military organizations, and multibillion-dollar companies**. Team members' backgrounds span executive leadership, advanced penetration testing, red teaming, exploit development, cryptography, cloud architecture, enterprise risk management, and secure software development, combining deep technical expertise with proven enterprise experience.

Collectively, the team holds some of the industry's most advanced security certifications, including **OSCE, OSEP, OSWE, OSCP, GXPN, CISSP, CRTE, and AWS Solutions Architect**, giving it the expertise to assess sophisticated threats, architect resilient systems, and develop innovative security technologies.

Beyond cybersecurity, Q Branch brings complementary experience ranging from **combat leadership in the U.S. Army** to advanced research in emerging technologies such as **quantum computing**, combining operational discipline, strategic thinking, and technical innovation with the ability to solve complex challenges in high-stakes environments. The team's combined experience in artificial intelligence, secure communications, security automation, and enterprise infrastructure provides a strong technical foundation for building and scaling Sekur's next-generation cybersecurity products and services.

Built to Scale with Account Growth and International Expansion

Sekur is preparing for planned account additions among **C-suite executives, government agencies, and defense organizations**, and for expansion into government and defense markets internationally. C-suite, government, and defense buyers typically require evidence of rigorous, ongoing security testing before and after deployment. **Q Branch gives Sekur the dedicated capacity to support that growth while maintaining highly secure systems** for its existing enterprise, government, defense, and executive clients. Planned account additions and expansion are subject to market conditions and client decisions, and there can be no assurance that they will be achieved.

Sekur offers government clients two deployment models. In the Swiss-hosted model, the service runs on Sekur-controlled hardware in Swiss data-center facilities. In the on-premises model, Sekur installs and configures the platform on approved hardware within the organization's own facilities, giving the client full data sovereignty and sole control over its keys and data.

Share Issuance and Stock Option Grant

The shares and stock options described below are shares and stock options of **Sekur Private Data Ltd., the publicly traded parent company** (OTCQB: SWISF | CSE: SKUR | FRA: GDT0). In consideration for services already rendered by Q Branch, Sekur Private Data Ltd. has issued **6,000,000 common shares**. Sekur Private Data Ltd. has also granted **2,000,000 stock options** to Q Branch for services to be rendered through December 31, 2028. Each option is exercisable to acquire one common share of Sekur Private Data Ltd. at **US$0.10** for a period of two years from the date of grant. Key terms are as follows:

Item	Detail
Issuer	Sekur Private Data Ltd. (publicly traded parent company)
Common shares, services already rendered	6,000,000 common shares of Sekur Private Data Ltd.
Stock options granted	2,000,000 stock options of Sekur Private Data Ltd.
Option exercise price	US$0.10 per common share
Option term	Two (2) years from the date of grant
Services covered by the options	Services to be rendered through December 31, 2028
Scope of services	Security; code monitoring and improvements; new feature roll-out and quality control

The common shares and stock options of Sekur Private Data Ltd., and any common shares issued on exercise of the options, are subject to the policies of the Canadian Securities Exchange and applicable securities laws, including any applicable hold periods.

Sekur Core Communications Solutions

Sekur delivers secure communications that work within and beyond the Sekur network, operating independently of conventional telecom infrastructure to reduce exposure to interception, SIGINT collection, traffic analysis, metadata exploitation, and hostile surveillance in contested environments. No Sekur solution data-mines or location-tracks its users.

All solutions are built on proprietary architecture with zero reliance on Big Tech, meeting the privacy, security, and OPSEC requirements of intelligence agencies, defense and federal organizations, military commands, diplomatic missions, government agencies, executives, and professionals handling CUI and other sensitive, mission-critical information. Deployments are supported by on-premises infrastructure options for full data sovereignty, mission assurance, and sole control over keys and data.

SekurOne — Encrypted Voice/Video, Email, Messaging, and VPN

A fully encrypted communications platform engineered on proprietary HeliX data transfer architecture, purpose-built to defeat telecom network tracing, resist Pegasus-style malware intrusion, and support CUI handling requirements. SekurOne is designed for defense and federal officials, military commanders, government leaders, and executives conducting confidential, operational, or sensitive conversations where standard carrier-based voice and video platforms present unacceptable interception and exploitation risk.

Call-by-Invite capability via SMS or SekurSend email ensures controlled access and eliminates unsolicited contact. Each user is assigned a unique Sekur ID for identity management, with no phone number required — preserving user privacy across all voice and video communications.

SekurMail — Secure Business and Executive Email

An enterprise- and government-grade encrypted email platform designed for defense and federal agencies, military commands, senior government officials, C-suite executives, and organizations handling confidential and operationally sensitive communications, including CUI correspondence. Built on proprietary architecture with zero Big Tech dependencies and no metadata tracking, SekurMail keeps sensitive communications private between sender and recipient.

Key capabilities include SekurSend/SekurReply for secure delivery to non-Sekur recipients without exposing sender identity or message content; full message delivery control and audit capability; encrypted file transfer; custom domain support for organizational integration; and active protection against phishing, social engineering, and Business Email Compromise (BEC) attacks targeting corporate and administrative networks.

SekurMessenger — Secure Team Messaging and Collaboration

A secure messaging platform providing end-to-end encrypted text, file transfer, voice messages, and collaboration capabilities for defense, military, government, and executive teams coordinating operational and mission-sensitive information, including CUI material. Features include self-destructing messages, encrypted file transfers, and compliance-grade archiving for recordkeeping and audit requirements.

Cross-network secure communications with non-Sekur users are supported via Chat-by-Invite, enabling secure coordination with coalition partners, external agencies, and field elements without compromising the network. Each user is assigned a unique Sekur ID for identity verification and contact authentication, with no phone number required.

SekurVPN — Enterprise Network Security and Identity Protection

An enterprise-grade Virtual Private Network leveraging proprietary HeliX encryption technology, engineered to provide secure internet access, identity obfuscation, and traffic protection for defense organizations, military and federal personnel, government agencies, and executives operating across remote, traveling, deployed, forward, or untrusted network environments.

SekurVPN maintains zero data logging, ensuring no record of user activity exists that could be exposed through legal process, network compromise, or third-party collection. It is built for defense, government, and executive use cases — including protection of traffic associated with CUI and operationally sensitive workflows — where standard commercial VPN solutions present unacceptable privacy and security risk.

SekurRelay — Executive-Level Secure Email Integration

An enterprise-grade secure email relay solution enabling domain splitting, which allows organizations to establish secure communications at the executive, board, or senior staff level without requiring full organizational migration or infrastructure overhaul.

SekurRelay removes one of the most significant barriers to large-scale defense, government, and enterprise deployment, enabling phased adoption that protects command leadership, flag officers, and the highest-value personnel and communications immediately while broader organizational rollout proceeds. It is designed for defense and government organizations, regulated industries, and enterprises requiring rapid, low-friction elevation of communications security at the command and executive tier, including environments handling CUI communications.

About Sekur Private Data

Sekur Private Data is a Swiss-hosted cybersecurity, defense communications, and privacy solutions provider, offering a secure suite of tools to protect governments, defense and federal agencies, businesses, and individuals from unauthorized access and cyber threats. With capabilities such as SekurOne, SekurMail, SekurMessenger, and SekurVPN, Sekur provides a reliable and secure means of digital communication and data storage for Controlled Unclassified Information (CUI), classified-adjacent and civilian communications use, grounded in Swiss privacy standards with on-premises infrastructure for government agencies, allowing for data sovereignty. Sekur sells its solutions through its website **www.sekur.com**, approved distributors and telecommunications companies globally, and through the **U.S. General Services Administration (GSA) Multiple Award Schedule (MAS), Contract No. 47QTCA18D0089** serving governments, defense institutions, federal agencies, businesses, and consumers worldwide. Sekur's main sales operations are in Miami, USA.

Contact

Alain Ghiai
President and Chief Executive Officer
Sekur Private Data
Email: investors@sekur.com
Tel: +1.305.347.5114
https://sekur.com/en/company/investors

Follow Sekur on X and LinkedIn.

To find out more about Sekur, visit https://sekur.com

Forward-Looking Information

This news release contains certain forward-looking information within the meaning of applicable Canadian securities laws ("forward-looking statements"). All statements other than statements of present or historical fact are forward-looking statements. Forward-looking statements are often, but not always, identified by the use of words such as "anticipate", "achieve", "could", "believe", "plan", "intend", "objective", "continuous", "ongoing", "estimate", "outlook", "expect", "project" and similar words, including negatives thereof, suggesting future outcomes or that certain events or conditions "may" or "will" occur. These statements are only predictions. These statements reflect management's current estimates, beliefs, intentions and expectations; they do not guarantee future performance. Sekur cautions that all forward-looking statements are inherently uncertain, and that actual performance may be affected by a number of material factors, many of which are beyond Sekur's control. Such factors include, among other things: the ability of Q Branch to maintain the Company's security, monitor and improve its code, and roll out new features with appropriate quality control; the ability of Q Branch to detect and defend against AI-driven intrusion and other evolving threats; the Company's ability to scale its systems and maintain their security; the timing and achievement of planned C-suite, government, and defense account additions; the Company's ability to expand into government and defense markets internationally; the exercise or non-exercise of the stock options; risks and uncertainties relating to the future of the Company's business; the success of marketing and sales efforts of the Company; the projections prepared in house and projections delivered by channel partners; the Company's ability to complete the necessary software updates; increases in sales as a result of investments in software development technology; consumer interest in the Products; future sales plans and strategies; reliance on large channel partners and expectations of renewals to ongoing agreements with these partners; anticipated events and trends; the economy and other future conditions; and other risks and uncertainties, including those described in Sekur's prospectus dated May 8, 2019, filed with the Canadian Securities Administrators and available on www.sedarplus.ca. Accordingly, actual and future events, conditions and results may differ materially from the estimates, beliefs, intentions and expectations expressed or implied in the forward-looking information. Except as required under applicable securities legislation, Sekur undertakes no obligation to publicly update or revise forward-looking information.