Sekur Private Data Receives US$3.4 Million per Year Quotation Request from African Government for 1,000 Command Bundle Licenses, 200 SekurOne Accounts and 200 Sekur Tactical Mobile Routers

A possible on-premises server installation for 2,500 to 5,000 users, valued at US$6 million to US$12 million per year including hardware and maintenance, is also under discussion

---

MIAMI, FL — October 27, 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 received a quotation request from a government in Africa for 1,000 licenses of the Sekur Command bundle, at a retail price of US$1,800 per license per year, or US$1.8 million per year; 200 SekurOne accounts, at a retail price of US$3,000 per account per year, or US$600,000 per year; and a minimum of 200 SekurVPN + STMR (Sekur Tactical Mobile Router) units at a retail price of US$5,000 per unit per year, or US$1 million, for a total quotation value of US$3.4 million per year in recurring annual fees. **The request also covers a possible on-premises server installation for between 2,500 and 5,000 users, which, including hardware and maintenance, would represent US$6 million to US$12 million per year.** Discussions with the government are at an advanced stage.

Under the terms of a non-disclosure agreement and the secrecy and compliance requirements that govern the engagement, Sekur is not permitted to disclose the name of the country or the government department or agency involved. The quotation request does not constitute a binding order, and there can be no assurance that a definitive agreement will be concluded or that its final terms will match the quotation. The Company will provide further updates, to the extent permitted, as discussions progress.

“Receiving a quotation request of this size from a government in Africa is an important milestone for Sekur,” said Alain Ghiai, Founder and CEO of Sekur Private Data. “**Governments want sovereign communications that they control, with no dependence on Big Tech platforms or on telecom networks they do not own**. Our Command bundle, SekurOne, the Sekur Tactical Mobile Router, and a possible on-premises installation together give this government a path to secure its leadership communications first, and then extend that protection to thousands of users and hundreds of locations.”

“Discussions are advanced, and we are **working closely with the client on technical and commercial terms.** Being able to deploy on-premises, inside the client’s own facilities and under its sole control of keys and data, is exactly what sovereign government clients are asking for. We look forward to updating our shareholders as soon as we are permitted to.”

The Quotation: Command Bundle and SekurOne Licensing and On-Premises Deployment

The quotation request is for 1,000 licenses of the Sekur Command bundle at Sekur's retail price of US$1,800 per license per year, or US$1.8 million per year. On top of the Command bundle, the government has requested a quotation for 200 SekurOne accounts at Sekur's retail price of US$3,000 per account per year, or US$600,000 per year. SekurOne is Sekur's fully encrypted voice and video, email, messaging and VPN platform, built on Sekur's proprietary HeliX data transfer architecture and requiring no phone number. The government is also considering an on-premises server installation for between 2,500 and 5,000 users, which, including hardware and maintenance, would represent US$6 million to US$12 million per year and would allow the deployment to grow well beyond the initial 1,000 licenses.

The itemized quotation is as follows. All fees are annual:

Item	Quantity	Unit retail price	Value
Sekur Command bundle licenses (annual)	1,000	US$1,800 / year	US$1,800,000 / year
SekurOne accounts (annual)	200	US$3,000 / year	US$600,000 / year
SekurVPN + STMR (Sekur Tactical Mobile Router) units, one per location (minimum, annual)	200	US$5,000 / year	US$1,000,000 / year
Total quotation (annual recurring fees)			**US$3,400,000 / year**
Potential on-premises server installation, 2,500 to 5,000 users, including hardware and maintenance (under discussion, not included in total)	2,500–5,000 users	—	US$6,000,000–US$12,000,000 / year

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.

SekurVPN + STMR (Sekur Tactical Mobile Router): A Controlled Network Boundary for Mobile Teams

In addition to the Command bundle licenses and SekurOne accounts, Sekur has quoted a minimum of 200 SekurVPN + STMR (Sekur Tactical Mobile Router) units, one per location, at a retail price of US$5,000 per unit per year, or US$1 million per year. The STMR provides gateway-level protected connectivity for a defined team operating from a temporary or non-secure location. Instead of relying on a separate VPN client being installed and activated on every device, **STMR moves the protected route to the local network boundary: authorized devices connect to a single managed local network, and their traffic is routed through the gateway's HeliX tunnel to the selected Swiss-hosted or on-premises Sekur environment.**

The STMR operating model follows four steps: Deploy, where the approved gateway is placed and configured for the operating location; Join, where authorized devices connect to the managed local network; Route, where the gateway sends connected traffic through the HeliX tunnel; and Control, where gateway and operator access is managed according to deployment policy. Because traffic passes through a controlled sovereign gateway, local carriers and internet service providers are prevented from analyzing or tracing operational data flows.

STMR is designed for temporary mission locations, partner facilities, mobile operational teams, and incident and continuity sites, as well as for field personnel connecting from hotels, transit hubs, and other networks the organization does not control.

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 possibility that the quotation request described in this news release does not result in a definitive agreement, or that the number of licenses, users or locations, the deployment model, or the value of any final agreement differs materially from the quotation; 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.