Sekur Private Data to Attend the ASCIA 2026 Fall Conference as a Silver Corporate Sponsor, Represented by Former U.S. Capitol Police Chief Steven A. Sund

Sekur will present its Swiss-hosted and on-premises sovereign secure communications solutions to the senior executives of state criminal investigative agencies from across the United States

---

MIAMI, FL — October 20, 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 will attend the 2026 Fall Conference of the Association of State Criminal Investigative Agencies ("ASCIA") as a Silver Corporate Sponsor. The conference takes place October 22–24, 2026, at the Renaissance Orlando at SeaWorld in Orlando, Florida. Sekur will be represented by Steven A. Sund, Sekur's Special Advisor, Federal, State & Local Law Enforcement. Chief Sund was a member of the Metropolitan Police Department of the District of Columbia for 25 years, where he was commander of the department's Special Operations Division. He joined the United States Capitol Police in 2017, becoming its Chief in 2019.

Founded in 1978, ASCIA is a non-profit association whose members are the senior executives of statewide criminal investigative agencies, including independent state bureaus of investigation and state police agencies with criminal investigation responsibilities, with membership covering almost every state in the United States. ASCIA promotes professionalism and helps its member agencies deliver high-quality, efficient services to their citizens through information sharing, interagency cooperation, policy development on national and regional issues, and biannual conferences that include training for agency leadership.

"We are very pleased to support ASCIA as a Silver Corporate Sponsor and to have Chief Sund represent Sekur in Orlando," said Alain Ghiai, Founder and CEO of Sekur Private Data. "State criminal investigative agencies handle some of the most sensitive information in law enforcement every day, from active case files to the identities of informants and undercover officers. Chief Sund understands those operational realities first-hand, and he is the right person to show agency leaders how Sekur can protect their communications."

"ASCIA brings together the leaders who set the direction for criminal investigations in nearly every state. Being in the room with them, as a sponsor, is how we intend to build long-term relationships with state law enforcement, alongside our work with federal and local agencies."

Steven A. Sund: Decades of Law Enforcement Leadership

Steven A. Sund was a member of the Metropolitan Police Department of the District of Columbia for 25 years, where he rose to the rank of Deputy Chief and served as commander of the department's Special Operations Division. He joined the United States Capitol Police in 2017 and became its 10th Chief in 2019. He is a Congressional Gold Medal recipient. As Sekur's Special Advisor, Federal, State & Local Law Enforcement, Chief Sund advises the Company on the secure communications needs of law enforcement agencies at every level of government and supports Sekur's engagement with agency leadership.

At the ASCIA Fall Conference, Chief Sund will meet with directors, superintendents, and senior executives of state criminal investigative agencies to discuss how Sekur's solutions can secure investigative, operational, and command-level communications.

Secure Communications for State Criminal Investigations

State criminal investigative agencies lead and support investigations into homicide, narcotics, organized crime, public corruption, human trafficking, cybercrime, and other major crimes, often through multi-jurisdictional task forces that include federal, state, and local partners. The information they exchange, including case details, evidence, surveillance plans, and the identities of informants, witnesses, and undercover personnel, must be protected from interception and exposure. A compromised call, email, or message can endanger lives, compromise an investigation, or alert a target.

Communications carried over conventional telecom networks and consumer messaging platforms can be traced, intercepted, or exploited, and many rely on phone numbers that reveal the identity and location of the user. State and local government networks also remain frequent targets of ransomware, phishing, and Business Email Compromise attacks.

Sekur's solutions, including SekurOne, SekurMail, SekurMessenger, SekurVPN, and SekurRelay, are designed for exactly these requirements. They operate independently of conventional telecom infrastructure, do not data-mine or location-track their users, and require no phone number. SekurRelay allows agencies to secure the communications of command staff and investigative leadership first, without a full organizational migration, and on-premises deployment options give agencies full data sovereignty and sole control over their keys and data. Sekur's solutions are also available to government buyers through the U.S. General Services Administration (GSA) Multiple Award Schedule (MAS).

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: 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.