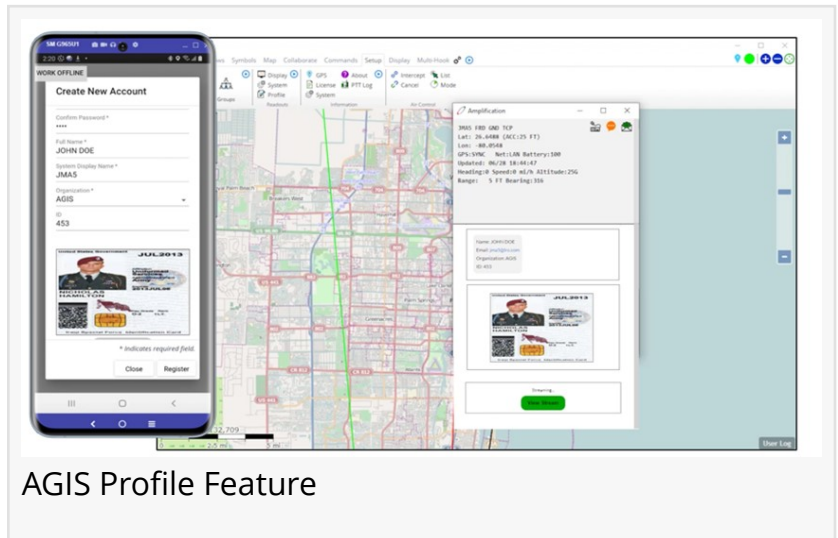# AGIS Software Tackles the Hidden Danger of Captured Military Devices

The Profile Feature Assures You Know Who's Who On The System

JUPITER, FL, UNITED STATES, November 12, 2024 /EINPresswire.com/ -- In today's modern battlefield, technology is both a boon and a bane. Military digital devices like smartphones and Tablet PCs have become indispensable tools for communication, navigation, and intelligence. However, these devices also pose operational risks when they fall into the hands of hostile

AGIS Profile Feature

forces. The capture of such devices can lead to severe security breaches, compromising not only the safety of individual soldiers but also the integrity of military missions and larger scale operations.

> ... the implementation of sophisticated safeguards is essential for maintaining the integrity and security of military operations."
>
> *Malcolm K. Beyer, Jr. CEO*

The Risks of Captured Devices

When military devices are captured by hostile forces, the consequences can be significant. These devices often contain sensitive information, including troop movements, strategic plans, and communication logs. Hostile forces can exploit this information in several ways:

l.   Location Tracking: Smartphones, in particular, can be tracked through their GPS and cellular signals. This allows enemies to pinpoint the location of troops, making them vulnerable to targeted attacks.

2. Data Interception: Captured devices can provide access to encrypted communications and classified documents. This information can be used to anticipate and counter military strategies.

3. Psychological Warfare: The knowledge that their communications and locations are compromised can demoralize troops and disrupt their operations.

AGIS C5ISR: A Technological Shield

To mitigate these risks, the AGIS C5ISR (Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance) is an advanced software solution designed to enhance situational awareness and ensure the security of military operations through real-time data integration and live audio/video confirmation.

Key Features of AGIS C5ISR

1. Real-Time Data Sharing: AGIS C5ISR allows for the instantaneous transmission of live video feeds, sensor data, and other critical information to the command center. This ensures that commanders have up-to-date situational awareness and can make informed decisions quickly.

2. Enhanced Situational Awareness: By integrating data from multiple sources, including drones, ground sensors, and satellite imagery, AGIS C5ISR provides a comprehensive view of the operational environment. This holistic approach enables the identification of threats and the assessment of risks more effectively.

3. Live Video Confirmation: One of the standout features of AGIS C5ISR is its ability to use live video feeds to confirm the identity and status of blue forces (friendly troops). This feature ensures that only authenticated and authorized personnel are recognized as legitimate members of the forces, reducing the risk of infiltration by hostile elements.

How Live Audio/Video Confirmation Works

All users have an active Profile attached to their user symbol. This includes their Full Name, Profile Photo, Email, Display Name, Organization, Number, Position and Phone Number. Any user in the system can click on another user to view this information and verify their identity. If it is suspected that an enemy is posing as the owner of any device, any network participant can ask another user to use their device camera to live-stream a selfie video. This video can then be compared - in real-time - to their Profile photo to verify their identity.

In an era where technology is both a critical asset and a potential vulnerability, the implementation of sophisticated safeguards is essential for maintaining the integrity and security of military operations. By leveraging real-time data sharing, enhanced situational awareness, and live audio/video confirmation, AGIS C5ISR ensures that blue forces are authenticated, authorized, and legitimately recognized, thereby safeguarding military operations and personnel. AGIS User Profiles Feature is just one of the many security checks built into the AGIS C5ISR system to guard against deception.

To see a full overview of AGIS LR Security features, go to:
https://www.agisinc.com/videos/SecurityVideo.mp4

For information on this system, contact Cap Beyer at beyerm@agisinc.com or at 561-744-3213.

To get the latest version of any of our Thick client apps, go to www.agisinc.com/download

To try our Web client system, go to either www.liferingmilitary.com _or_
www.liferingfirstresponder.com

Made in the USA by American Citizens
-

Malcolm "Cap" Beyer
Advanced Ground Information Systems (AGIS)
+1 561-744-3212
beyerm@agisinc.com