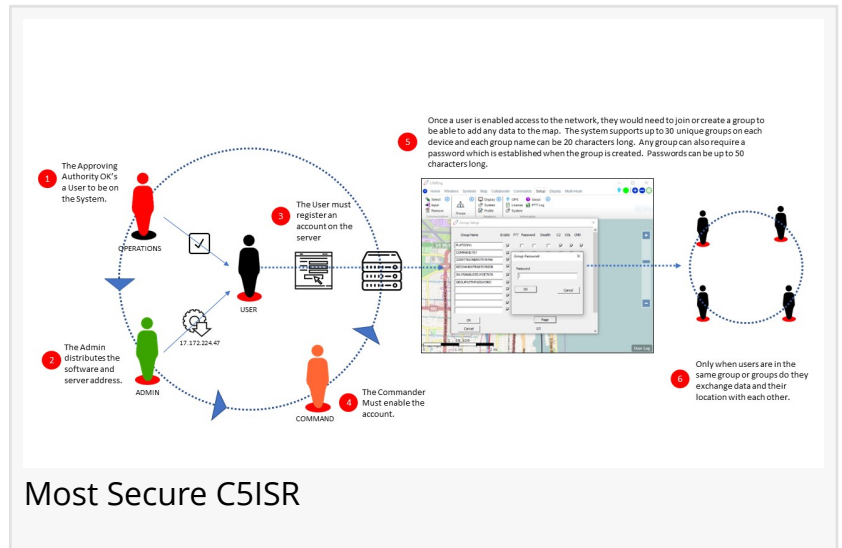


# Advanced C5ISR Security of AGIS LifeRing

*Multiple Layers of Cyber, Data, and Authentication Security for Military Operations*

JUPITER, FL, US, September 30, 2022 /EINPresswire.com/ -- AGIS – Advanced Ground Information Systems, the makers of LifeRing Multi Domain Data Link ([MDDL](#)) Software, have designed a C5ISR Common Operating Picture (COP) to be the most comprehensive and easy to use Command and Control system in the world. With the latest version Release 6.03, it is now the most secure.



From the on-boarding of C5ISR users, to organizing users into groups, to encrypting the data and communications exchanged by all these users, security has been built-in at every level.



All data that is transmitted is first protected using AGIS proprietary message exchange formats, which are known to AGIS and only one U.S. entity."

*Malcolm K. Beyer, Jr.*

All on-boarding users must initially be approved by their approving authority in order to have a licensed copy of the software and have a registered account on the AGIS Server. Both the software installation and the server access information have to be issued to each user by an Administrator or gatekeeper to the system.

Using a simplified but secure process, all user accounts can be set as email validation or through the manual approval/enabling of the account by the Administrator.

Once a user is granted login access, they then need to join or create a group in order to use the system and to be able to add any data to the map-oriented user interface. The originator of a group can establish a Group Name, up to 20 characters, and a password up to 50 characters, to create a group. No user can join an existing group unless they know the precise group name and the password. Many groups can be registered on the server and the system will support as many as 30 unique group names on each PC, Tablet, or handheld device. Only when users are in the same group or groups can they exchange data and location with each other.

Group Security Access safeguards may be installed to

- a. limit data to the upper levels of a command structure
- b. limit data to only a select personnel, e.g., Intelligence
- c. limit the security level of data shared across allied militaries

The formation of groups may be based on echelon, command structure, mission, security level or location.

Groups can be set at the user's local level or at the next command level. New or additional groups can be set up at each level of a given organizational structure, with security access safeguards installed to securely seal off upper levels of the command structure.

Depending on permissions and authorities, a user within each Group can select what Group they join, and this will determine the data they will be authorized to receive.

Built into the system is an optional setting for stealth operation. When this setting is selected, a user's location will no longer be visible to other group members. All operational data added or modified on the map by other users, messages, chat, and PTT communications will remain visible on the map display. The user device in Stealth Mode however will not transmit location data.

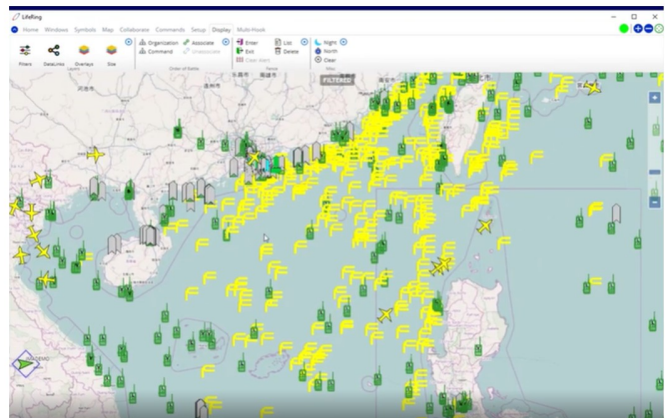
Additional security:

In the event a user is compromised or if the device is lost or stolen, the device in question may be removed from the network in two different ways.

At the server level, a user can be temporarily blocked from the network thereby forcing them to login again.

AGIS LR Security Features	
1. User on-boarding to be authenticated by an Administrator	✓
2. Login to specific IP address for access to AGIS LR app	✓
3. After login, user is required to join or create a Group	✓
4. Unique Group name can be up to 20 characters	✓
5. System supports up to 30 Group names on each PC/handheld device	✓
6. Originator may secure Group access with a 50-character password	✓
7. Only users in same group(s) can exchange data and location with each other	✓
8. Formation of Groups may be based on <ul style="list-style-type: none"> <li>- echelon</li> <li>- command structure</li> <li>- mission</li> <li>- security level</li> <li>- or location</li> </ul>	✓
9. Group Security Access safeguards can be installed to: <ul style="list-style-type: none"> <li>a. limit data to upper levels of a command structure</li> <li>b. limit data to only select personnel, e.g., Intelligence</li> <li>c. limit the security level of data shared across allied militaries</li> </ul>	✓
10. All data transmitted is first protected by AGIS proprietary message exchange formats known to AGIS and only one U.S. entity	✓
11. Data is AES 256-bit encrypted prior to transmission	✓
12. With Harris and other U.S. military radios, data is further encrypted by the radio prior to transmission using U.S Type 1 encryption	✓
13. With Motorola radios, the data is encrypted using AES 256-bit encryption, using a different encryption key	✓
14. At the server, data transmissions are integrated with XQ Messaging to meet Zero Trust NIST 800-171 advanced encryption, routing, and data management compliance requirements	✓
15. If user is compromised or if a device is lost or stolen, the device can be removed from the network temporarily or permanently, by the Administrator	✓
16. Additional security features not for press release	✓

### AGIS LifeRing Security



AGIS Processing Commercial Satellite ELINT from South China Sea

All operational data added or modified on the map by other users, messages, chat, and PTT communications will remain visible on the map display. The user device in Stealth Mode however will not transmit location data.

A user can also be permanently blocked from the network. This action disables the user's account from being able to login. Access privileges can only be re-enabled at the server level with the action of the Administrator.

All data that is transmitted is first protected using AGIS proprietary message exchange formats, which are known to AGIS and only one U.S. entity. The data is then encrypted prior to transmission using AES 256-bit encryption.

In areas where communications are done using Harris or other U.S. military radios, the data is further encrypted by the radio itself prior to transmission using [U.S. Type-1 encryption](#). When using Motorola radios, the data is further encrypted using AES 256-bit encryption, but with a different encryption key.

At the server level, AGIS data transmissions have been integrated with XQ Messaging to meet [Zero Trust](#) NIST 800-171 advanced encryption, routing, and data management compliance requirements. Whenever required LifeRing will use XQ Messaging's Zero Trust, wherein the data being transmitted is encrypted using separate keys for either the second or third time.

If a secure State of the Art Low Cost C5ISR system is of interest, please contact [beyerm@agisinc.com](mailto:beyerm@agisinc.com)

Malcolm K. Beyer, Jr.  
Advanced Ground Information Systems (AGIS)  
[beyerm@agisinc.com](mailto:beyerm@agisinc.com)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/593141411>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 Newsmatics Inc. All Right Reserved.