AGI Security Compliance Statement

Securing our products and protecting our customers is of the highest priority. AGI has implemented processes and standards to protect the integrity of our source code and our sensitive data. As a vendor to the United States Government, AGI is required to comply with the Defense Federal Acquisition Regulation Supplement (DFARS) clauses 252.204-21/7008/7012. These clauses stipulate security standards for the safeguarding of Government information and for cyber incident reporting. AGI also complies with domestic and international privacy regulations such as the General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA).

AGI has instituted security controls and policies, based on standards established in NIST Special Publication 800-171. These standards govern how information is protected on AGI's computer systems and how access to AGI's network and facility is managed and monitored. In compliance with DFARS clause 252.204-7020, AGI's self-assessment score in the Supplier Performance Risk System (SPRS) is currently 110 out of a possible 110 for the entire enterprise.

AGIs security and privacy standards cover the following areas:

Controlled Access to AGI Facilities and Networks
Everyone is required to wear an ID badge in plain view while inside the AGI Exton Headquarters. All visitors must sign in and wear a visitor badge. Access to areas where AGI's products are developed is restricted to US Citizens.

Controlled Access to AGI Computer Systems
Only authorized personnel may access AGI's computer systems and network. AGI's product development environment is isolated and only accessible by authorized product development personnel. All AGI computers used in support of a contract require multi-factor authentication for all user accounts and privileged accounts.

Restrictions on Storage of Customer and Contract-Related Data
All documents and data related to a customer contract are stored in designated network locations and approved portable storage devices. Such locations require credentials for access. Credentials are issued only to those who need to know about the contract to perform their job at AGI. Access is determined by the Project or Contract Manager assigned to the contract.

Restrictions on Sharing of CUI, FOUO and Personal Data
Controlled Unclassified Information (CUI) and For Official Use Only (FOUO) data are only shared with personnel who have been approved under the terms of the contract with the customer. The Project Manager maintains a list of approved personnel. Personal data is collected, retained and destroyed as directed by the GDPR and domestic privacy laws.

Confidentiality
Information about Government contracts that AGI participates is only shared as permitted in the Contract or by the Project Manager.

Specific Protections for AGI Source Code
Our software development network, which is the only computing network where our source code resides, is compartmentalized. Code development is entirely isolated without direct access to other networks or the Internet. AGI's pre-release software build and testing process provides another layer of security. Our process includes steps that will detect security vulnerabilities, injections, viruses, spyware and trojans, including:

- Peer code reviews
- Configuration and change control management with SSL-secured communications
- Daily automated regression testing to detect unintentional changes to mitigate the risk of injection
- Continual static code analysis for all daily builds using Coverity, FxCop and PREfast for specialized analysis
- Virus scanning of all customer deliverables

Scanned media is never replicated, and unscanned media cannot enter the development network without approval from a development security officer.

Revised 10/29/21