ThinGap Trade Compliance Statement
Revision date: January 2021

General Position

ThinGap's electric brushless DC motor components are commercial in nature and commercially developed.

For trade and export compliance, ThinGap considers it products to be classified as EAR99 and subject to the US Commerce Department's Export Administration Regulations. The bases of this determination are the following:

I. that its products are not listed with a specific Export Control Classification Number (see additional statement below) on the Commerce Control List, and

II. its products are not ITAR-restricted as a defense article in the US Defense Department's US Munitions List (USML).

In one case, where two commercial products were modified for use in a Government-funded communications satellite program, those variants of ThinGap products are classified as ECCN 9A515.x.

Since ThinGap has determined it products are not defense articles as defined by the USML, the Company is not ITAR Registered with the US State Department's Directorate of Defense Trade Controls.

Foreign Sales and Compliance

In all cases of foreign sales, for US-Trade Compliance, ThinGap requires a use-statement confirmation from end customers about the intended use of the product, per the following:

> *"The products and data manufactured by ThinGap may not be used in the design, development, production or use of nuclear, chemical or biological weapons or missiles."*

In addition, the Company has a Standard Operating Procedure that provides added safeguards and Trade Compliance as part of contract and purchase order reviews, including use of the US International Trade Administration's Denied Persons List for customer screening and consideration of Government flow-down requirement or restriction called out by the customer-issued contract or purchase order.

Acknowledgement and Procedures

ITAR restricts and controls the export and import of defense and military related technologies. Within the ITAR is the US Munitions List that provides a list of all items controlled within the ITAR. Any person who engages in the business of either manufacturing or exporting defense articles or furnishing defense services is required to register with the Directorate of Defense Trade Controls.

ThinGap acknowledges the national importance of ITAR and the overall need for Trade Compliance. The Company conducts annual employee training in support of Trade Compliance and can provided additional safeguards that might be required by Government-programs or requirements.

In those cases where access to ITAR-controlled documents is required in support of a qualified Customer project, the following Transfer and Control Procedure is required. This Procedure is based on industry established standards and NIST (The National Institute of Standards and Technology) SP 800-53 defined standards and guidelines for Federal Agencies to architect and manage their information security systems for the protection of Government and citizen's private data.

Transfer and Control Procedure

ThinGap's Transfer and Control Procedure requires that only when necessary should ITAR-Controlled Data (defined as technical data that is export-controlled) be accepted and handled. Internally, only U.S. Persons with a need-to-know should be allowed to access Controlled Data.

Controlled Data should be saved on a secure network, with adequate access restrictions in place to insure only U.S. Person and those needing access have it. The goal of NIST 800-53 compliance is based on several basic principles to data security:

I. Discover and Classify Sensitive Data – locate and secure all sensitive data at the time of access or receipt;

II. Map Data and Permissions - identify users, file permissions and determine who has access;

III. Manage Access Control - deactivate stale users, remove any global access groups, implement privileges;

IV. Monitor Data, File Activity, and User Behavior – audit, monitor for insider threats, malware, misconfigurations and security breaches, detect security vulnerabilities and remediate.

Transfer of Controlled Data should never be sent via unsecure electronic mail, instead a secure file sharing solution should be used. In no cases should usernames or passwords of authorized parties be shared and controlled data or systems housing them should never be accessed using an unauthorized computer or device.

Once Controlled Data is no longer needed or required for its original intended use, it should be properly deleted or destroyed. Periodic reminders should be sent to all holders or potential holders of Controlled Data to consider items to be deleted or destroyed.

ThinGap's Management is responsible for the proper handling and use of Controlled Data. Any breach or errors in the application of the Transfer and Control Procedure should be reported to Management immediately. Reviews and consideration for changes to this Procedure should be as need and ongoing in nature.

[END]