

Honeywell Federal Mfg. & Technologies, LLC
14520 Botts Road
D/011 MS 01.3.E14
Kansas City, MO 64147

export@kcnc.doe.gov

Date: May 6, 2020

Subject: Supplier Expectations in Handling Export Controlled Information

Dear Valued Supplier:

As a supplier for Honeywell Federal Manufacturing & Technologies, LLC (FM&T) we are providing you with our expectations of your company's responsibilities relative to the handling and protecting of controlled unclassified information which may be provided to your company.

In accordance with the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR) and the Atomic Energy Act (AEA), it is illegal to release articles, software or technical data found on the export control lists to foreign persons, where ever located, without authorization from the applicable U.S. government agency.

Articles or technical data Honeywell FM&T may provide to suppliers identified as export controlled are for use in the United States and by U.S. persons only. A supplier shall not release, sell, export, resell, divert, duplicate, dispose of or otherwise transfer any article or technology identified as export controlled to foreign persons, regardless of location.

Technical data identified as Export Controlled Information/Official Use Only will be marked on the bottom of the first page of the technical data and/or the bottom of each page of the document containing ECI/OUO information. Additionally, the purchase order will contain an export control statement advising you as the supplier when an article, software, technology or service is export controlled.

A supplier shall have written procedures which describe how the company internally securely protects and handles export controlled articles/information restricting access to foreign persons. At a minimum the procedures should include the following: Access, Storage, Electronic transmission, and destruction policies.

ACCESS: A supplier shall only allow U.S. persons to have access to FM&T export controlled articles and/or technical data, and only U.S. persons will be allowed to perform any work on behalf of FM&T.

- Precautions shall be taken to prevent unauthorized individuals from overhearing the conversation, observing the material, or otherwise obtaining the information.
- Operating procedures and physical security measures should be designed to protect export controlled items from inadvertent release or disclosure to foreign persons or other unauthorized third parties. Foreign persons who are not permanent resident aliens (green card holders) are not allowed access to export controlled items.
- Although we understand your business need to advertise your technical capabilities, suppliers may not use items or information produced for or provided by FM&T for this purpose. This includes advertising posters, display cases and supplier websites. FM&T products and information should not be on display during a visitor tour.

In addition, suppliers are not allowed to reference FM&T, the Kansas City National Security Campus, or the Nuclear or Nuclear Weapons Industry in their web-based or printed materials.

STORAGE of FM&T ECI/OUO information shall be maintained within a secure area.

- Secure areas may include a locked receptacle such as a file cabinet, desk drawer, overhead furniture credenza system, or similar locked compartment. ECI/OUO can also be stored in a room or area that has sufficient physical access control measures (guard, cipher lock, card reader, etc.) to afford adequate protection and prevent unauthorized access.
- Servers shall be hosted in the United States and maintained by U.S. persons. A supplier shall maintain adequate controls in its information technology system to protect against unauthorized access, disclosure and transfer of ECI/OUO technical data and software.

TRANSMISSION of ECI/OUO information will be sent electronically through a secured method of transmission. (e.g. Email encryption or authorized users of Web Exchange)

- Supplier is also responsible to send ECI/OUO information through secure method when transmitting electronically.

DESTRUCTION of ECI/OUO information including gerber files and electronic storage media, when no longer needed, may be accomplished by shredding into strips, burning, pulping, or pulverizing beyond recognition or reconstruction. After destruction, material may be disposed of with normal waste.

- Export controlled articles scrapped, failed inspection or defective parts will require demilitarization (DEMIL) rendering useless the article. Supplier who does not have the ability to DEMIL process ability on site should contact FM&T to obtain an export control approved recycling company or return to FM&T.

SITE INSPECTION: FM&T shall conduct on-site security inspections of the supplier's facilities and ensure documented access control operating policies restricting foreign person access are in place. FM&T and the supplier agree to establish dates for those activities that are mutually satisfactory to each party.

A supplier is responsible to flow down foreign person restricted access control requirements to their subcontractors. It is the responsibility of the supplier to select a subcontractor who can securely protect and handling the ECI/OUO information that may be shared.

Please contact the Compliance Team in the Legal Department export@kcncs.doe.gov with any questions regarding suppliers export control responsibilities.