1. EXPORT CONTROLLED INFORMATION/OFFICIAL USE ONLY (ECI/OUO) HANDLING (Clause C-01.01) (May 2023)

If Seller receives a document or procurement marked "Export Controlled Information (ECI) or Official Use Only (OUO)" in the performance of its work, the following instructions are provided to assist in the proper handling of that OUO document.

a. **'Export Controlled Information/Official Use Only' or ECI/OUO** is marked on the bottom of the first page of the document and/or the bottom of each page of the document containing ECI/OUO information. By designating all or a portion of the document as ECI/OUO, the originator has determined this information is to be disseminated only to U.S persons.

b. **ACCESS to ECI/OUO documents and items** are restricted from foreign person's access, including supplier's foreign person(s) employees, consultants, visitors and or subcontractors.

Supplier shall ONLY allow U.S. persons deemed to have a business need, to have access to Buyer ECI/OUO documents and/or items, and only U.S. persons will be allowed to perform any work on behalf of Buyer. Precautions are to be taken to prevent unauthorized individuals from overhearing the conversation, observing the material item, or otherwise obtaining the information. Foreign persons, who are permanent resident aliens (green card) and deemed to have a business need, are authorized access to ECI/OUO documents and items. Buyer reserves the right to conduct periodic reviews of the Seller's records.

The supplier shall have a written procedure that prohibit the access of foreign persons to ECI/OUO articles/information, including flowing down ECI/OUO requirements to sub-tier suppliers.

c. **STORAGE of ECI/OUO information** must be in a secured method. Example: locked receptacle such as a file cabinet, desk drawer, overhead furniture credenza system, or similar locked compartment or locked room. The information can also be stored in a room or area that has sufficient physical access control measures (guard, cipher lock, card reader, etc.) to prevent inadvertent release to unauthorized access.

Servers shall be hosted in the United States and maintained by U.S. persons. Supplier shall maintain controls in its information technology system to protect against unauthorized access, disclosure or transfer of ECI/OUO technical data and software. To store ECI/OUO on a computer, the system must prevent access from foreign persons. This includes, but not limited to, foreign person employees who are not permanent residents and foreign owned parent or subsidiary offices.

d. **TRANSMISSION of ECI/OUO** information will be in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container must bear the complete name and address of the sender and the intended recipient with "To Be Opened By Addressee Only" on the outside. Information may be mailed using first class, express, certified or registered mail.

Electronic transmission (fax or email) of ECI/OUO requires use of encryption or other secure approved methods of transmission.

e. **DESTRUCTION of ECI/OUO information**, including documents and electronic storage media, when no longer needed, may be accomplished by shredding into strips no wider than 1/4 inch, burning, pulping, or pulverizing beyond recognition or reconstruction. After destruction, material may be disposed of with normal waste." ECI/OUO items (product) rejected or returned for credit must be rendered useless and destroyed.

The supplier shall have a written procedure for the destruction of the following ECI/OUO articles/information including documents, electronic media and materials when no longer needed/usable. Destruction shall make said articles unrecognizable and subsequently disposed using normal waste processing.