

Solicitation #:

Project Title:

REQUEST FOR ACCESS TO NASA DOCUMENTS CONTAINING EXPORT CONTROLLED EAR, ITAR AND/OR SBU INFORMATION

Receipt and use of NASA documents containing export controlled EAR or ITAR information is restricted to U.S. Citizens and/or U.S. Permanent Residents with a Green Card.

The NASA documents containing export controlled EAR and ITAR information fall under the following security requirements: Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR) as defined in NPR 2190.1, "NASA Export Control Program", and Sensitive But Unclassified (SBU) regulations as defined in NPR 1600.1, "NASA Security Program Procedural Requirements". As a recipient and user of these documents you are required to comply with these requirements.

Initial: _____

Users of NASA documents containing export controlled EAR or ITAR information need to be aware of their responsibility to the sensitivity and protection requirements of EAR, ITAR and SBU documentation. **Users handling this documentation shall limit its access to authorized users only (Firms incorporated in the US and U.S. Citizens and/or a U.S. Permanent Resident with a Green Card).** When unattended, this documentation must be stored in a locked file cabinet, locked desk drawer, a locked credenza, or similar locked compartment. It can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by unauthorized users. **Emails shall not contain EAR, ITAR or SBU information.** EAR, ITAR or SBU information can only be transmitted via first class mail, courier, encrypted FTP, encrypted HTTP, or secure fax.

Initial: _____

EAR, ITAR and/or SBU documentation that is no longer needed shall be removed from IT systems. Hard copy materials shall be destroyed by shredding, burning, pulping, pulverizing, or destroyed in other similar methods that preclude unauthorized disclosure. Electronic storage media shall be sanitized appropriately by overwriting or degaussing, or non-recoverable encrypted deletion.

Initial: _____

By requesting access to NASA documents containing export controlled EAR or ITAR information, you are acknowledging that you accept responsibility that any further distribution of this information, whether within your company or to potential suppliers or subcontractors, is performed within the restrictions of the EAR and ITAR.

Initial: _____

Contact Randy Gumke, Kennedy Space Center (KSC) Contracting Officer by telephone at (321) 867-3322, or by e-mail to randall.a.gumke@nasa.gov, if you have any questions concerning this form or anything else pertaining to the NASA procurement.

ACKNOWLEDGEMENT STATEMENT

Unauthorized use of the documents containing export controlled EAR or ITAR information to which I am granted access is a violation of Section 799, Title 18, U.S. Code; constitutes theft; and is punishable by law. I understand that individuals provided access to these documents and information must comply with the relevant US export control laws and regulations. I understand that my misuse of these documents and information may constitute grounds for administrative action and/or civil or criminal prosecution.

Your company's security department or corporate officer shall provide a certification on company letterhead to the Contracting Officer that: the identified person requesting access to these documents is an employee of the company and either a US citizen or lawful US permanent resident with a green card; all individuals provided access to such information will comply with the relevant US export control laws and regulations. This completed and signed access request form and the certification on company letterhead shall be submitted at the same time.

Last Name First Name Middle Initial

Telephone No. Email Address

Organization/Company Name Cage Code DUNS No.

Business Mailing Address (include Building and Room Number)

Yes No Yes, Expiration Date: No
U.S. Citizen If not a U.S. citizen, are you a permanent resident (Green Card Holder)

User Signature Date