Export Control Briefing
and
Non-Disclosure Agreement

CH2M HILL BWXT West Valley, LLC

Request for Proposal/Subcontract # _____

This project may involve the use of Export Controlled Information. As a result, the project invokes either the International Traffic in Arms Regulation (ITAR) under the jurisdiction of the Department of State, or the Export Administration Regulations (EAR) under the jurisdiction of the Department of Commerce.

It is unlawful under the ITAR to send or take Export Controlled Information out of the U.S.; disclose, orally or visually, or transfer Export Controlled Information to a foreign person inside or outside the U.S. without proper authorization. Under the ITAR or the EAR, a license may be required for foreign nationals to access Export Controlled Information. A foreign person is a person who is not a U.S. citizen or permanent resident alien of the U.S. The law makes no exceptions for foreign graduate students.

In general, Export Controlled Information means activities, items and information related to the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, operation, modification, demilitarization, destruction, processing or use of items with a capacity for military utility. Export Controlled Information does not include basic marketing information on function or purpose; general system descriptions; or information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It does not matter if the actual intended end use of Export Controlled Information is military or civil in nature.

Contractors and their employees may be held personally liable for violations of the ITAR and EAR. As a result, you should exercise care in using and sharing Export Controlled Information with others. Technical information, data, materials, software or hardware, i.e.; technology generated from this project, must be secured from use and observation by non-U.S. citizens. Both civil and criminal penalties may be imposed for unlawful export and disclosure of Export Controlled Information up to and including incarceration.

Security measures will be appropriate to the classification. Examples of security measures are (but not limited to):

- Project Personnel – Authorized personnel must be clearly identified.
- "Work-in-Progress" – Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
- Marking of Export Controlled Information – Export Controlled Information must be clearly identified and marked as Export Controlled. (It should be noted that there is a possibility that some information provided by the Government may not have been marked and care should be taken with any material that is suspected to be "Export Controlled").
- Work Products – Both soft and hardcopy data, notebooks, reports, and research materials should be stored in locked cabinets; preferably located in rooms with key-controlled access.
- Electronic or internal components – Such tangible items and associated operating manuals and schematic diagrams containing identified "Export Controlled" technology are to be physically secured from unauthorized access.

- Electronic communications and databases – Appropriate measures will be taken to secure controlled electronic information. Such measures may include: user ID, password control, or approved encryption technology. Database access may be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using a federally approved encryption technology.
- Conversations – Discussion about the project and its work products are limited to the identified contributing employees and subcontractors and are only in areas where unauthorized personnel are not present. Discussion with third party sub-contractors are only to be conducted under signed agreement that fully respect the non-U.S. citizen limitations for such disclosures.

Certification: I hereby certify that I have read and understand the information above and the attached *Requirements for Export Controlled Information*. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export Controlled Information to unauthorized persons. I further certify that I am a U.S. Citizen or a Permanent Legal Resident with appropriate clearances.

Name (Printed): _____

Signature: _____ Date: _____

Company: _____

Position: _____

Address: _____

_____

_____

Telephone: _____

Email: _____

REQUIREMENTS FOR EXPORT CONTROLLED INFORMATION

1. Export Controlled Information. ECI is any technical information determined to contain technical data, the export of which is restricted by:

   - 10 CFR 810, DOE Assistance to Foreign Atomic Energy Activities, or
   - 15 CFR 774, U.S. Department of Commerce (DOC) Export Administration
   - Regulations, Commerce Control List, Supplement 1, or
   - 22 CFR 121, U.S. Department of State (DOS) U.S. Munitions List, or
   - DOE export control guidance.

   If exported, ECI requires a technology export license or authorization under United States export regulations.

2. Non-Public Technical Data (NPTD). NPTD is technical data which is not publicly available and which is not specifically identified in 10 CFR 810, 15 CFR 774 - Supplement 1, or 22 CFR 121. The U.S. DOC requires an export license review prior to transferring NPTD to a foreign national (deemed export) or transferring NPTD out of the U.S.

3. Deemed Export. A domestic release of export controlled technology or source code to a foreign national who is not a person lawfully admitted for permanent residence in the United States (e.g., holder of a green card) or a protected individual (e.g., refugee) under the Immigration and Naturalization Act [8 USC 1324B (a) (3)].

4. Export. An actual shipment, transmission, or release of items, technology, or software out of the United States.

5. Release. Release occurs when NPTD or ECI leaves the bidder's control or is transferred to a foreign national.

6. Release of Technology or Source Code. Technology or source code is "released" for export through:

   a. Visual inspection by foreign nationals of U.S. - origin equipment and facilities;

   b. Oral exchanges of information in the United States or abroad; or

   c. The application to situations abroad of personal knowledge or technical experience acquired in the United States.

7. Technology. Specific information necessary for the development, production, or use of a product. The information takes the form of technical data or technical assistance.

   NOTE 1: Technical assistance -- May take forms such as instruction skills training, working knowledge, or consulting services.

NOTE 2: Technical assistance may involve transfer of technical data.

8. Technical Data. May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, and read-only memories.

9. Access. ECI access may be granted to bidder employees who are U.S. Citizens with established need-to-know in the performance of official or contractual duties. Foreign nationals may be given access to NPTD only after a need-to-know is established for the foreign national by DOE and an export license or authorization has been obtained from the appropriate U.S. agency (i.e., DOC, DOS, or DOE), if required. Export licenses or authorizations are for a specific technology and do not authorize access to any other technology without another specific EC review. DOE approval should be obtained prior to the release of ECI or NPTD to any foreign national no matter what form the technical data may take.

10. Originator. The originator of a document is responsible for the initial identification and protection of NPTD and ECI and must seek out an Export Control Reviewer to conduct a formal review if the information is being considered for release outside the DOE or to any foreign national. (Contact the Contracting Officer)

11. EC Reviewer. An individual, who by familiarization and/or experience is considered a subject matter expert, authorized to make a determination that equipment, material, or technical information is or is not export controlled. (Contact the Contracting Officer)

12. Marking Requirements. Products containing ECI must be clearly marked in accordance with the following procedures:

    a. The following statement must be marked on the cover or first page of any information product determined to contain ECI:

"EXPORT CONTROLLED INFORMATION"

Contains technical data whose export is restricted by statute. Violations may result in administrative, civil, or criminal penalties. Limit dissemination to U.S. citizens who are U.S. Department of Energy (DOE) employees or DOE contractors or employees of other U.S. Government agencies. The cognizant program manager must approve other dissemination. This notice shall not be separated from the attached document.

_____
Reviewer (Signature)

_____
Date

_____
Source Document

b. The bottom of each interior page determined to include ECI must be marked:

"EXPORT CONTROLLED INFORMATION"

c. Documents, faxes, e-mails, containing technical data being released to U.S. Government agencies and their contractors (U.S. citizens only) do not require an export control review if marked:

CONTAINS NON-PUBLIC TECHNICAL DATA
Requires Export Control Review Prior to Release to the Public or any Foreign National.

13. Physical Protection.

a. In Use. Any individual authorized access to ECI must maintain physical control over the matter to prevent unauthorized access to the information.

b. In Storage. ECI must be secured behind a locked door or in a locked container/desk when unattended; or in a method which would prevent/preclude unauthorized disclosure.

c. Information Systems.

- Password protected or on removable media
- With distribution restricted to those with established need-to-know
- Be clearly marked as appropriate

d. Transmission.

(i) Mail Transmission. ECI must be in a single sealed opaque envelope or wrapping and addressed to the recipient to include marking "TO BE OPENED BY ADDRESSEE ONLY." Packages may be sent as follows:

- Hand-carried
- U. S. Mail by First Class, Express, Certified, or Registered Mail
- Any commercial carrier (e.g., Federal Express, Emery, etc.) using signature service

(ii) Over Telecommunication Circuits:

ECI must be protected by approved encryption when transmitted off site by telecommunications services. ECI transmitted over public-switched broadcast communications paths (e.g., Internet) then the information must be protected by approved encryption.

e. Reproduction. Matter marked as containing ECI may be reproduced without the permission of the originator to the minimum extent necessary

consistent with need to carry out official duties and need-to-know as long the matter is not marked as "Dissemination Controlled." Any copy machine malfunctions must be cleared to ensure no ECI matter is left in the machine.

f. Destruction.

(i) The normal method for destroying documents containing ECI is by using a strip-cut shredder that outputs strips not exceeding ¼-inch wide. This may be done in workplace, if a strip shredder is available.

(ii) Computer storage media such as floppy disks, ZIP, JAZ cartridges, hard drives, CDs, etc., containing ECI must be destroyed by shredding/chipping, crushing or burning or returned to the Contracting Officer.

Prior to sending bidder equipment or media containing DOE information to an offsite vendor for repair or warranty credit or redeployment, the DOE information must be cleared by the bidder.