**Appendix A**

**Export Control Review**

**PROJECT INFORMATON**



**PROJECT INFORMATION**

**Project Title**

**Project/Contract/Proposal #**

**Sponsor**

**Principal Investigator**

**Campus Address**

**School Department/Division**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SECTION I. PROJECT ANALYSIS** | | | | |
|  | **Sanctioned Countries, Entities and Persons** | | **YES** | **NO** |
| **1.** | Does the project in any way involve either of the following: | |  |  |
| a. | a country subject to US economic sanctions |  |  |  |
| b. | a person or entity designated by the US Government as a Specially Designated National or a  Blocked Person (SDN) | |  |  |
| *For the current list of sanctioned countries, please visit:* [*http://www.treasury.gov/offices/enforcement/ofac/programs/index.shtml.*](http://www.treasury.gov/offices/enforcement/ofac/programs/index.shtml)  *The Specially Designated National or a Blocked Person (SDN) can be viewed at:*  [*http://www.treasury.gov/offices/enforcement/ofac/sdn/index.shtml.*](http://www.treasury.gov/offices/enforcement/ofac/sdn/index.shtml)  If you answered “**YES**” to questions **1(a)** or **1(b)**, please contact the Office of Sponsored Programs before proceeding with the activity.  If the answer is “**NO**” to both of these questions, please proceed to the next question. | | | | |
|  |  | **Public Domain** | **YES** | **NO** |
| **2.** | Does the project  **solely** involve information or technologies that are in the ‘public domain’, (e.g., published, patented, or generally accessible to the public)? | |  |  |
| If the answer is “**YES**,” please skip to question #**4** and then question #**8** below. In summary, if no encryption software is involved and the activity does not involve a boycott-related request, then you must contact the Office of Sponsored Programs only if you know or have any reason to believe that the public domain item, technical data, or software to be shipped, transmitted or transferred will be used to support design, development, production, stockpiling or use of nuclear, chemical or biological weapons or missiles.  If you answered “**NO**” to question #2, please proceed to the next question. | | | | |
|  | **Fundamental Research** | | **YES** | **NO** |
| **3.** | Do the terms of the proposal, application or award, or the terms of the contract or research agreement, contain **any** of the following: | |  |  |
| a. | Restrictions on publication (e.g., sponsor approval rights or prepublication review) beyond a brief review for patent protection and/or inadvertent release of confidential/proprietary information? | |  |  |
| b. | Restrictions on the participation of foreign persons (e.g., sponsor approval required for participation of non-U.S. persons, explicit restrictions on participation by persons or entities based on their country of nationality, prohibitions on access by non-US persons to project information, or prohibition on hiring non-US persons)? | |  |  |
| c. | Requirement to keep information confidential (e.g., requires the PI to sign a non-disclosure or a confidentiality agreement, or otherwise addresses the use of proprietary information or security concerns) | |  |  |
| d. | Permission for the sponsor to claim resulting research information as proprietary or trade secret (i.e., sponsor’s intent to retain proprietary interest over the results)? | |  |  |
| e. | “Export controlled,” “ITAR controlled” or similar marks anywhere on the documents (e.g., RFP, SOW) or any other references to US export control regulations? | |  |  |
| If you answered “**NO**” to ALL of the questions (a)-(e), the “fundamental research” exclusion will apply to information resulting from the research.  *It is important to note that this exemption:*  • *does allow for the release of such information to a foreign person*  ***in*** *the United States; but*  • *does not authorize transmission or transfer of items, software or technical data outside the United States.*  *If the project contemplates or involves such export activity, or if you anticipate that the activities of this project will involve foreign persons who may need to use controlled equipment or software in the United States, completing the remainder of the questionnaire will assist you in determining whether a license is required for such export or whether the transfer of “use” technology is involved.*  If you answered **“YES”** to any of the questions (a) – (e) the Fundamental Research exclusion does not apply. In addition, if you answered “**NO**” to question #**2** above, you should contact the Office of Sponsored Programs in: (i) properly classifying the information or technology involved, (ii) determining the scope of applicable restrictions under US export controls and (iii) defining your obligations in conducting the research. You may be asked to complete questions **4**-**7** below as well as the Certification on the Handling of Export Controlled Information (also referred to as Appendix B of the Export Control Policy). | | | | |
| **SECTION II. TRANSFERS, CONTROLS, AND LICENSING** | | | | |
| **Encryption Items** | | | **YES** | **NO** |
| **4.** | Does the project involve shipping, transmitting or otherwise transferring encryption software (in source code or object code)? | |  |  |
|  | If the answer is **“NO”**, please proceed to the next question.  If the answer is **“YES”**, please contact the Office of Resource Management, Operations and  Emergency Preparedness before proceeding with the activity. | |  |  |
|  | **Transfers or Exports** | | **YES** | **NO** |
| **5.** | Does the project involve shipment, transmission, or transfer of any item, information, or non- encryption software outside the US? | |  |  |
| If the answer is **“NO”**, please skip to question **#8**.  If the answer is **“YES”**, please proceed to the next question. | | | | |
|  | **ITAR / USML** | | **YES** | **NO** |
| **6.** | Is the item, software or information being shipped, transmitted or transferred subject to the International Traffic in Arms Regulations (ITAR) as a Defense Article or Technical Data listed on the U.S. Munitions List (USML) or otherwise specifically designed, developed, configured, adapted or modified for a military application? | |  |  |
| *The U.S. Munitions List (USML) is located at:*  [*http://www.pmddtc.state.gov/regulations\_laws/documents/official\_itar/ITAR\_Part\_121.pdf*](http://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf) *.*  If you answered “**YES**,” it is likely a license will be required to ship, transmit or otherwise transfer the item, software or technical data outside the United States. You should contact the Office of Sponsored Programs before proceeding.  If the answer is **“NO”**, please proceed to the next question. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Commerce Control List and EAR99** | | | |
| The Bureau of Industry and Security (BIS) maintain the Commerce Control List (CCL) which includes items (i.e., commodities, software, and technology) subject to the export licensing authority of BIS. In order to complete the next question, you must review the CCL to determine the category in which the item(s) used in this project will be classified. | | | |
| *The CCL is available at* [*http://www.access.gpo.gov/bis/ear/ear\_data.html#ccl,*](http://www.access.gpo.gov/bis/ear/ear_data.html#ccl) *Part 774, Cat. 0-9.* | | **CCL** | **EAR99** |
| **7.** | Is the item, software or information being shipped, transmitted or transferred listed on the Commerce Control List (CCL) of the Export Administration Regulations (EAR) or is it classified in the “basket” category EAR99? |  |  |
| If you have determined that the item, software or information being shipped, transmitted or transferred is classified in the basket category “EAR99”, please skip the next question and refer to the guidance information in the shaded text box below. | | | |
| **Transfer of Use** | | **YES** | **NO** |
| a. | If you are dealing with the CCL-listed information or software, has it been published, patented or generally accessible to the public in any form? |  |  |
| If your answer is **“YES”** the CCL-listed information or software is exempt from the EAR restrictions as “publicly available” information or software (with the exception of certain encryption software, which remains subject to the EAR and is covered by question 4 above).  If your answer is **“NO”** and you are dealing with the CCL-listed information or software that is  **not** publicly available and/or you are dealing with a CCL-listed item, the following must be determined:  1) the level of EAR controls applicable to that item, information or software (by determining the proper Export Control  Classification Number (ECCN) on the CCL);  2) the country of destination for such item, software or information and/or the nationality/citizenship of a foreign person who will receive such information or software in a third country; and  3) whether a license under the EAR is required,  4) or whether a license exception may apply.  You should contact the Office Sponsored Programs if you need assistance in making these determinations.  **EAR99** items generally consist of low-technology consumer goods and do not require a license in many situations. However, if your proposed export of an EAR99 item is to a country subject to US economic sanctions, to an end-user on a U.S. Government Restricted Party List, or in support of a prohibited end-use, you may be required to obtain a license.  ***Important note:***  *You will also need to advise UNA of the following information prior to engagement:*  • *whether you know or have any reason to believe that the item, technical data, or software to be shipped, transmitted or transferred will be used to support design, development, production, stockpiling or use of nuclear, chemical or biological weapons or missiles;*  • *any “red flags” are present (for a list of EAR red flags, please review* [*http://www.bis.doc.gov/enforcement/redflags.htm);*](http://www.bis.doc.gov/enforcement/redflags.htm)%3B) *or*  • *any of the parties to the contemplated transaction appear on any U.S. Government*  *“restricted party” lists*  *The lists are available at:*  [*http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm*](http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm)*)* | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Boycotts** | | **YES** | **NO** |
| **8.** | Does the project, or the contemplated activity, involve a boycott-related request? |  |  |
| For more information on anti-boycott compliance requirements, please review <http://www.bis.doc.gov/ComplianceAndEnforcement/AnitboycottCompliance.htm>  If the answer is **“YES”**, please contact the Office Sponsored Programs before proceeding (you should not provide any response to such request without obtaining prior legal guidance). | | | |

**Signature Date**

**APPENDIX B**

**CERTIFICATION ON THE HANDLING OF EXPORT CONTROLLED INFORMATION Overview**

The activity/project identified below will involve the receipt and/or use of technical data that is controlled under U.S. export control laws: the Export Administration Regulations (“EAR”), enforced by the

Commerce Department’s Bureau of Industry and Security, or the International Traffic in Arms Regulations (“ITAR”), enforced by the State Department’s Directorate of Defense Trade Controls (DDTC).

**EAR**

EAR controls the export and re-export of equipment, software and technical data that serve commercial or “dual use” purposes. The prohibition on the export or “deemed export” (i.e., disclosure to a foreign person in the United States) of technical data controlled under the EAR is determined on a country-by-

country basis, depending on the country of destination (or the foreign person’s country of citizenship/nationality) and the level of controls imposed by the EAR on particular equipment, software

or technical data. As a result, it is unlawful to export technical data from the US to a foreign country or to disclose technical data in or outside the US to foreign persons who are nationals/citizens of countries for

which an export license is required as a condition of making such exports and disclosures.

**ITAR**

ITAR controls the export and re-export of equipment, software, and technical data, and the provision of services, that are primarily military in nature (i.e., specifically designed, developed or modified for a

military application). It is unlawful to send ITAR controlled technical data to *any* foreign persons outside the United States or to disclose – in written, oral or visual form - ITAR-controlled technical data to  *any* foreign persons *in* or *outside* the United States unless one of several exclusions applies or the State

Department has issued a license authorizing the disclosure or export of the technical data to specific foreign persons.

**Obligations**

Recipients of export controlled technical data may be held personally liable for disclosures to

unauthorized foreign persons. As a result, members of the University community must take reasonable measures to prevent the disclosure to and use and access of export controlled technical data by unauthorized, unlicensed foreign persons. What qualifies as reasonable depends on the circumstances.

**Safeguards**

Examples of measures that members of the University community should consider adopting include clearly marking “controlled” technical data that is controlled, identifying personnel who may lawfully

access the technical data, storing hard copies of controlled technical data in locked cabinets or desks, securing access to electronic copies of and communications containing controlled technical data by

passwords, user ids, or other controls; storing technical data in a single location; making only that number of copies of technical data as is necessary, and requiring all persons with lawful access to controlled technical data to sign this certification.

**Penalty**

Individual liability for the disclosure of controlled technical data to unauthorized foreign persons under

the ITAR can reach up to $1 million per violation and 10 years imprisonment for willful violations, and civil fines up to $500,000 per violation. A university found to be in violation of ITAR regulations can be debarred from contracting with the government and could lose its export privileges.

Liabilities under the EAR may involve fines greater of $1 million for each willful violation. Individuals can be fined up to $1 million and imprisoned for 20 years, or both. Civil penalties can reach up to

$250,000 or 2 times the value of the transaction, whichever is greater, per violation. The university itself

and individual faculty, staff and researchers can also lose their privilege to export and may be debarred from contracting with the federal government.

**Certification on the Handling of Export-Controlled Information**

I certify that I am familiar with the University of North Alabama’s Export Control Policy and the export control issues summarized above, and I have read and understand this certification.

I understand that I could be held personally liable if I unlawfully disclose export controlled technical data to foreign persons and I agree to take reasonable measures to prevent unauthorized foreign persons from having access to or using any export controlled technical data I may receive under the contract identified below.

I agree to take appropriate security measures and to contact The Office of Sponsored Programs before making any type of disclosure of controlled technical data to any foreign person.

Signature of Member/Researcher: Date

Printed Name of Member/Researcher: Division / Department:

Research Project Title: \_\_\_\_\_\_\_\_\_\_ Proposal ID or Contract # \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sponsor:

**Please attach a copy of the Export Control Review to this document and return to: Office of Sponsored Programs, Bibb Graves Room 208.**