



THE GEORGE
WASHINGTON
UNIVERSITY
WASHINGTON DC

Responsible University Official:

Associate VP, Resource Management,
Operations and Emergency Preparedness

Responsible Office: Resource
Management, Operations and Emergency
Preparedness

Origination Date: October 1, 2004

EXPORT CONTROL POLICY

**(LIMITING DISTRIBUTION AND SHARING OF INFORMATION, TECHNOLOGY AND
COMMODITIES BOTH INTERNATIONALLY AND DOMESTICALLY)**

Policy Statement

It is the policy of the university to comply with U.S. export control laws. Export control laws restrict certain types of information, technologies, and commodities that can be transmitted overseas to individuals, including U.S. citizens, or made available to foreign nationals on U.S. soil.

It is the responsibility of faculty and administrators to be aware of and comply with these laws and the university's written instructions and procedures.

Reason for Policy/Purpose

The export of certain items, technologies, software and services is regulated for reasons of national security, foreign policy, prevention of the spread of weapons of mass destruction and for competitive trade reasons. Prior written authorization (a "license") from one or more U.S. government agencies will be required to carry out certain sponsored research or other educational activities involving specified technologies or certain countries, if an exemption or exclusion is not available.

Export control laws restrict the shipment, transmission or transfer of certain items, software, technology and services from the U.S. to foreign countries, as well as "deemed exports," which are releases of controlled technology and software source code to foreign nationals located in the U.S.

Although many of the university's activities are exempt from export control laws, some activities may be restricted. Failure to comply with these laws exposes both the employee and the university to severe criminal and civil penalties (fines and prison sentences) as well as administrative sanctions (loss of research funding and export privileges).

Criminal penalties for unlawful export and disclosure of information in violation of U.S. export control laws may include fines up to \$1 million and/or imprisonment up to 20

EXPORT CONTROL POLICY

years. Civil penalties can be assessed up to \$250,000 or 2 times the value of the transaction, whichever is greater, for each violation. The university and the individual(s) involved also may lose their ability to export in the future.

Who Needs to Know This Policy

Faculty, staff and students

Table of Contents	Page #
Policy Statement	1
Reason for Policy/Purpose	1
Who Needs to Know This Policy.....	2
Table of Contents	2
Policy/Procedures	2
Website Address	5
Contacts.....	6
Definitions.....	6
Related Information	7
Appendices.....	7
Who Approved This Policy	7
History/Revision Dates	7

Policy/Procedures

I. OVERVIEW

The Department of State, through its International Traffic in Arms Regulations (ITAR) of the Directorate of Defense Trade Controls (DDTC), and the Department of Commerce, through its Export Administration Regulations (EAR) of the Bureau of Industry and Security (BIS), have implemented regulations governing export of certain technologies, information, and software. The U.S. export controls also apply to “re-exports” of items, software and technology subject to U.S. law from one foreign country to another. In addition, the Department of Treasury, through its Office of Foreign Assets Control (OFAC), maintains targeted economic sanctions programs that restrict or prohibit a wide range of export and other transactions which may include educational services involving designated countries, entities and individuals.

Before engaging in activities that involve an export, members of the university community must understand and identify any potential export limitations. A few examples of export controls ‘triggers’ include:

- Where Foreign Persons will participate in the research;
- Where GW will partner with a foreign company;

EXPORT CONTROL POLICY

- Where GW hosts foreign visiting scholars for the purpose of research that involves certain specified technologies subject to export controls;
- Where equipment needed for experiments or research abroad will be exported (i.e., shipped or accompanying the researcher/faculty member), including, for example, laptops, GPS equipment, other hand-held mobile devices, etc., or any device that contains encrypted software.

Many university activities are eligible for one of the EAR, ITAR, or OFAC exclusions, meaning that no license will be required. However, when a research or educational activity involves an export, GW must document its analysis of export control issues, including the availability of any exclusion or exemption.

The export control analysis should be undertaken with the assistance of the Office of Resource Management, Operations, and Emergency Preparedness (RMOEP) in the Medical Center, which has been delegated university-wide authority in this area. It is important to note that if a license will be required this analysis must be done prior to engaging, or agreeing to engage in the activity because the process for obtaining U.S. government approval is lengthy.

In some cases, GW may decide not to accept funding for research containing export controls or restrictions, including but not limited to when there is insufficient time to obtain a license or to take appropriate measures to handle properly export-controlled information.

If anyone employed by, acting on behalf of, or associated with the university receives information identified as “export controlled,” the information may not be disclosed to any “Foreign Person,” until the export control analysis has been completed to determine licensing requirements, if any, for such information. In addition, if an anticipated GW research or educational activity involves a country subject to U.S. government sanctions, the faculty member or researcher also will need to consult with GW’s Office of the Senior Vice President and General Counsel before entering into any negotiations or agreements involving, or before traveling to, such countries.

For detailed information about export control ‘triggers,’ activities that may present export-control issues, and these exclusions (e.g., Fundamental Research, Educational Information, Published Information and Software, and the exclusion for Full-Time University Employees) see *Guidance: Understanding Export Controls at GWU*, available from RMOEP at www.gwumc.edu/orm.

Members of the university community must understand their obligations under ITAR, EAR and OFAC regulations and promote compliance with these regulations. Criminal and civil penalties for unlawful export and disclosure of information in violation of U.S. export control laws may be assessed against individuals and institutions and may include the following:

EXPORT CONTROL POLICY

- **ITAR:** Criminal penalties can reach up to \$1 million per violation and 10 years imprisonment for individual willful violations. Civil penalties imposed upon departments, agencies, and officials can reach 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 privilege.
- **EAR:** Criminal violations by the university can incur penalties up to \$1 million for each willful violation. For individuals, these penalties can reach up to \$1 million or 20 years imprisonment, or both, per violation. Civil penalties for both the university and individuals can reach up to \$250,000 per violation, or two times the value of the export, whichever is greater. These violations can also result in a denial of export privileges as well as other potential collateral penalties.
- **OFAC:** Penalties will range depending upon the sanction regime in question. Criminal violations by the university can reach up to \$1 million, and criminal penalties for individuals can reach \$1 million or 20 years in prison, or both. Civil penalties can be imposed up to \$250,000 per violation, or two times the transaction in question, or both.

The university will assist any member of the university community in complying with export control laws, including pursuing licenses from U.S. Government agencies, where appropriate. However, the primary responsibility rests with the faculty/staff member and/or researcher, as the individual most informed about the contemplated project.

II. SUMMARY OF EXPORT CONTROL COMPLIANCE PROCEDURES

A. Review – Guidance: Understanding Export Controls at GWU

This guidance document is intended for the members of the university community to promote understanding of export controls regulations and the procedures designed to promote university compliance. It provides detailed explanations of the export controls regulations and their legal limitations, and will provide examples of export triggers and export-controlled activities. This guidance document is available from RMOEP at www.gwumc.edu/orm.

B. Complete - Record of Export Control Review Questionnaire (Appendix A)

The university has developed a questionnaire entitled *Record of Export Control Review*, an internal document to assist members of the University community in assessing U.S. export control issues in general, and whether a particular research project or contemplated activity would qualify for an exemption. Faculty/staff members and/or researchers should contact RMOEP for assistance with Appendix A, and to receive additional information regarding possible export control issues. In all situations, the questionnaire should be completed one (1) to six (6) months before the contemplated activity to afford sufficient time for the export control issues to be addressed in a timely manner. It is important to note that if an export license is required, commencement of the activities could be delayed.

EXPORT CONTROL POLICY

C. Implement Access Controls – Complete a *Certification on the Handling of Export-Controlled Information* (Appendix B)

If the project or activity involves input data that is export-controlled, but the research results remain eligible for the fundamental research exemption, the Principal Investigator (PI) will be primarily responsible for implementing and maintaining appropriate access controls so that a Foreign Person who is a part of the team does not have access to information that he/she is not authorized to receive. The faculty member/researcher will be required to attest to implementation of such controls by completing a *Certification on the Handling of Export-Controlled Information* (see Appendix B), also an internal GW document.

D. Obtain Export Licenses, Where Applicable

If a faculty/staff member and/or researcher determines, with the assistance of the university, that a particular project or activity is subject to export controls and no exemption is available, the faculty member/researcher is responsible for securing the items, software or technology against disclosure or transfer to any Foreign Person, within or outside the United States, until a license or other authorization is obtained. Also, the faculty/staff member and/or researcher will be required to complete the *Certification on the Handling of Export-Controlled Information* (see Appendix B).

Securing the appropriate licensing is a complex process and may take up to six (6) months. When an export license is required, the faculty member/researcher will notify RMOEP and his/her department will be primarily responsible for preparing the required license application and supporting materials to obtain the appropriate license under the ITAR, EAR, or OFAC regulations. All license applications will be submitted through RMOEP.

All requests for licenses from OFAC will be handled in conjunction with the Office of the Senior Vice President and General Counsel.

E. Review Additional Relevant University Policies

Members of the university community should be familiar with other university policies that may require additional procedures. For example:

1. [Policy on Classified Research](#)
2. [Compliance with U.S. Laws when Conducting University Activities Overseas](#)

Website Addresses for This Policy

[GW University Policies](#)

Contacts

Subject	Contact	Telephone
Questions	Office of Resource Management, Operations and Emergency Preparedness (RMOEP) www.gwumc.edu/orm	(202) 994-2312

Definitions

EAR	Export Administration Regulations, Department of Commerce
ITAR	International Traffic in Arms Regulations, Department of State
OFAC	Office of Foreign Assets Control, Department of Treasury
Export	Generally, an export means: (1) An actual shipment or transmission of items controlled under the EAR or ITAR out of the United States; (2) any written, oral or visual release or disclosure of controlled technology, information or software to a Foreign Person either in the United States or outside the United States; or (3) any actual use or application of controlled technology on behalf of or for the benefit of any foreign entity or person anywhere.
Deemed Export	Occurs when technology or software source code is released or transmitted to a Foreign Person within the U.S. including through a discussion with a foreign researcher or student.
Reexport	An actual shipment or transmission of items subject to export regulations from one foreign country to another foreign country. For the purposes of the U.S. EAR, the export or reexport of items subject to the EAR that will transit through a country or countries to a new country, or are intended for reexport to the new country, are deemed to be exports to the new country.
Foreign Person(s)	Both the EAR and ITAR define “Foreign Person” as any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the U.S. as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g. diplomatic missions), and anyone who is not a U.S. citizen, a lawful permanent resident of the U.S. (i.e., a “green card” holder) or who does not have refugee or asylum status in the U.S.

EXPORT CONTROL POLICY

Fundamental Research Exclusion Information arising during or resulting from basic or applied research in science or engineering where the results of the research are ordinarily shared with the scientific community, published in the public domain and made accessible to the public.

Related Information

Guidance: Understanding Export Controls at GWU: www.gwumc.edu/orm.

[Compliance with U.S. Laws when Conducting University Activities Overseas](#)
[Mobile Device Security Policy](#)
[Policy on Classified Research](#)

[Bureau of Industry and Security \(BIS\)](#)
[Export Administration Regulations \(EAR\)](#)
[International Traffic in Arms Regulations \(ITAR\)](#)
[Office of Foreign Assets Control](#)

Appendices

Appendix A **Record of Export Control Review**

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

Who Approved This Policy

Louis H. Katz, Executive Vice President and Treasurer
Donald R. Lehman, Executive Vice President for Academic Affairs
Beth Nolan, Senior Vice President and General Counsel
John F. Williams, Provost and Vice President for Health Affairs

History/Revision Dates

Origination Date: October 1, 2004
Last Amended Date: February 4, 2008
Next Review Date: March 31, 2013

This page left intentionally blank

EXPORT CONTROL POLICY

APPENDIX A

THE GEORGE WASHINGTON UNIVERSITY
OFFICE OF RESOURCE MANAGEMENT, OPERATIONS, AND
EMERGENCY PREPAREDNESS

RECORD OF EXPORT CONTROL REVIEW

Purpose

The purpose of completing the Record of Export Control Review is threefold:

1. Assist GW in properly classifying the information, technology, software or item involved,
2. Determine the scope of applicable restrictions under U.S. Export Controls,
3. Define your obligations in conducting the research.

This questionnaire was designed for use by any member of the university community in assessing U.S. export control issues in general, and to determine whether a particular research project or contemplated activity would qualify for an exemption. As the Principal Investigator (PI) for a research project, you are the person most qualified to provide information necessary to determine whether your research is subject to restrictions imposed by export control laws.

Instructions

Individuals who have identified export control triggers must complete the questionnaire and follow the procedures set forth therein. The Record of Export Control Review must also be completed by any member of the university who intends to transfer any item, software or technology outside the United States, even if the contemplated activity is unrelated to a particular research project.

For additional information and guidance, please review the Export Control Policy for a summarized explanation of export control laws, or visit www.gwumc.edu/orc.

PROJECT INFORMATION			
Project Title			
Project/Contract/Proposal #			
Sponsor			
GWU Member/Principal Investigator			
Campus Address			
School		Department/Division	
Phone		Fax	Email

EXPORT CONTROL POLICY

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)		
<p><i>For the current list of sanctioned countries, please visit: 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.</i></p> <p>If you answered “YES” to questions 1(a) or 1(b), please contact the GWU Office of the Vice President and General Counsel immediately, before proceeding with the activity.</p> <p>If the answer is “NO” to both of these questions, please proceed to the next question.</p>			
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)?		
<p>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 Senior Vice President and General Counsel 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.</p> <p>If you answered “NO” to question #2, please proceed to the next question.</p>			
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?		

EXPORT CONTROL POLICY

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 Resource Management, Operations and Emergency Preparedness to assist GW 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)?		
<p>If the answer is “NO”, please proceed to the next question.</p> <p>If the answer is “YES”, please contact the Office of Resource Management, Operations and Emergency Preparedness before proceeding with the activity.</p>			
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?		
<p>If the answer is “NO”, please skip to question #8.</p> <p>If the answer is “YES”, please proceed to the next question.</p>			
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.pmdtic.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 Resource Management, Operations and Emergency Preparedness before proceeding.

If the answer is “**NO**”, please proceed to the next question.

EXPORT CONTROL POLICY

Commerce Control List and EAR99		
<p>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.</p>		
<p>The CCL is available at http://www.access.gpo.gov/bis/ear/ear_data.html#ccl, Part 774, Cat. 0-9.</p>		
7.	<p>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?</p>	
<p>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.</p>		
Transfer of Use		
a.	<p>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?</p>	
<p>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).</p> <p>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:</p> <ol style="list-style-type: none"> 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. <p>You should contact the Office of Resource Management, Operations and Emergency Preparedness if you need assistance in making these determinations.</p> <p>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.</p>		
Important note:		
<p><i>You will also need to advise GW of the following information prior to engagement:</i></p> <ul style="list-style-type: none"> • <i>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;</i> • <i>any “red flags” are present (for a list of EAR red flags, please review http://www.bis.doc.gov/enforcement/redflags.htm); or</i> • <i>any of the parties to the contemplated transaction appear on any U.S. Government “restricted party” lists</i> <p><i>The lists are available at:</i> http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm)</p>		

EXPORT CONTROL POLICY

	Boycotts	YES	NO
8.	Does the project, or the contemplated activity, involve a boycott-related request?		
<p>For more information on anti-boycott compliance requirements, please review http://www.bis.doc.gov/ComplianceAndEnforcement/AnitboycottCompliance.htm or GW’s Primer on Doing Business Abroad: U.S. Laws That Affect GW’s International Activities, at http://www.gwu.edu/~vpgc/pdf/Primer_on_Doing_Business_Abroad.pdf</p> <p>If the answer is “YES”, please contact the Office of Senior Vice President and General Counsel before proceeding (you should not provide any response to such request without obtaining prior legal guidance).</p>			

Signature _____ **Date** _____

EXPORT CONTROL POLICY

APPENDIX B

THE GEORGE WASHINGTON UNIVERSITY OFFICE OF RESOURCE MANAGEMENT, OPERATIONS, AND EMERGENCY PREPAREDNESS

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.

EXPORT CONTROL POLICY

Penalties

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.

Resources

For additional information on export controls at GWU, visit: www.gwumc.edu/orm. For information on the EAR, visit the Bureau of Industry and Security at: <http://www.bis.doc.gov/>. For information on ITAR, visit the Directorate of Defense Trade Controls at: http://www.pmddtc.state.gov/regulations_laws/itar_official.html. For information about the Office of Foreign Assets Control, visit: <http://www.treasury.gov/offices/enforcement/ofac/>. For information on the SDN list and U.S. economic sanctions, visit <http://www.treas.gov/offices/enforcement/ofac/sdn/index.shtml>.

Certification on the Handling of Export-Controlled Information

I certify that I am familiar with the GW University 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 Resource Management, Operations and Emergency Preparedness before making any type of disclosure of controlled technical data to any foreign person.

Signature of GWU Member/Researcher: _____ Date _____

Printed Name of GWU Member/Researcher: _____

Division / Department: _____

Research Project Title: _____

Proposal ID or GWU # _____ Sponsor: _____

Please attach a copy of the Export Control Review to this document and return to:
Office of Resource Management, Operations and Emergency Preparedness
Attn: Export Controls - Compliance
2300 Eye Street N.W., Suite 430

EXPORT CONTROL POLICY

Washington, D.C. 20037