THE UNIVERSITY OF ALABAMA AT BIRMINGHAM (UAB)
TECHNOLOGY CONTROL PLAN (TCP) CERTIFICATION

PART I

Individual Requesting and Responsible for TCP:		
Telephone Number		
E-mail Address		
Request Date		
Description of Controls (EAR/ITAR Category)		
Location(s) Covered by TCP (add additional rows if needed)	Building	
	Room(s)	
Project Personnel	List Name(s) below:	List citizenship(s) / Permanent Res. Status:
Personnel who will have access to export controlled subject matter (add additional rows if needed)		

Is sponsored research involved?	Yes/No
If yes, identify sponsor:	
OSP Link Number and projected end date of project	

Is a non-disclosure agreement involved?	Yes/No
If yes, identify the parties:	
Contact Information:	

Attachments:	Export Briefing and Certification Form(s) for each person subject to this TCP	
Approved:	_____ Marilyn C. Thomas, JD Director of Export Control and International Compliance AND: Michael A. Matthews, MPA, CPM Interim – Associate Vice President and Executive Director	_____ Date _____ Date

PART II
BRIEFING AND CERTIFICATION ON THE HANDLING OF EXPORT-CONTROLLED INFORMATION

This project involves the use of Export-Controlled Information. As a result, the project implicates either the International Traffic in Arms Regulations (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 application 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.

Researchers 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 unlicensed 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 involved. Examples of security measures are (but not limited to):

- Project Personnel – Authorized personnel must be clearly identified.
- Laboratory "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.
- Work Products – Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets; preferably located in rooms with key-controlled access.
- Equipment 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, SSL or other 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 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.
- Conversations – Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.

Department(s):
Research Project Title:

OSP No.

Sponsor:

Certification: I hereby certify that I have read and understand this Briefing, and that I understand and agree to follow the procedures outlined in the TCP. I understand that I could be held personally liable if I unlawfully disclose, regardless of form or format, Export-Controlled Information to unauthorized persons.

Signature: Date:

PART III

TECHNOLOGY CONTROL PLAN (TCP)

1) COMMITTMENT
The University of Alabama at Birmingham (UAB) is committed to export controls compliance. The Office of Sponsored programs is responsible for implementing technology control plans as applicable. The individual responsible for and committed to ensuring compliance with this TCP is [INSERT Name of Responsible Party].

2) BACKGROUND AND DESCRIPTION OF THE USE OF CONTROLLED ITEMS AND INFORMATION
[INSERT]

3) PHYSICAL SECURITY
[INSERT description of how equipment, technology, data and other controlled information will be shielded from unauthorized persons including descriptions of relevant security systems such as badging, escorts, visitor logs and other types of building access restrictions.]

4) INFORMATION SECURITY
Controlled data are categorized under the Data Classification Standard as Category I data. All project data and other related digital materials will be strongly password-protected and encrypted using commercially available encryption technology. Guidance on utilizing encryption as a means of protecting sensitive digital data can be accessed at http://main.uab.edu/Sites/it/policies/. The computer(s) on which this data will be stored shall not be connected to any networks. When this computer has reached its usable life, the hard drive will be forensically erased or destroyed using university hard drive destruction services.

[INSERT an outline of additional measures that will be taken to ensure information access controls that will be utilized to ensure the requirements are met including use of passwords and encryption protection. The data discard policy and relevant information technology policies and procedures should be included, as well as other plans for controlling access to controlled information. These procedures should address system backup and who will have access, transmission procedures, how computers on which sensitive digital data will be stored will be sanitized upon completion of the project, and other procedures necessary to provide the necessary security. Use of laptops for storage of this data must be justified and will only be approved with additional security procedures.]

5) PERSONNEL SCREENING
All personnel with access to the controlled technology and their nationality are listed in the TCP Certification Form. [INSERT any information on the type of background check and any additional required reviews that will be employed beyond the University's standard background check procedures for all employees.]

6) TRAINING AND AWARENESS
All personnel with access to controlled information on this project have read and understand the "Briefing and Certification on the Handling of Export-Controlled Information." Additional export control training for this project may be conducted by the Director of Export Control and International Compliance (ECO). The ECO also provides periodic training sessions to members of the UAB community. Additionally, all personnel with access to digital data/information stored on their university computer have read and agree to follow the UAB procedures for Protecting Sensitive Digital Research Data.

7) COMPLIANCE ASSESSMENT
As a critical component to the University's ongoing compliance monitoring, self-evaluation is an internal assessment process whereby procedures are reviewed and any findings reported to the ECO at mcthomas@uab.edu (205)996-2735, to the Empowered Official for export controls at www.uab.edu/exportcontrol. The ECO may also conduct periodic evaluations and/or training to monitor compliance of the TCP procedures. Any changes to the approved procedures or personnel having access to controlled information covered under this TCP will be cleared in advance by the ECO or the Empowered Official for export controls.

8) PROJECT TERMINATION
Security measures, as deemed appropriate, will remain in effect after the project has ended in order to protect the export-controlled information unless earlier terminated when the information has been destroyed or determined to be no longer export-controlled.