Master Technology Control Plan for Export Controlled Information

Georgia Tech Research Institute

Copies to:

Research Security Department (RSD)
dannie.lyvers@gtri.gatech.edu
al.concord@gtri.gatech.edu
terry.culver@gtri.gatech.edu
bill.gregory@gtri.gatech.edu

Information Systems Development (ISD)
jeff.jenkins@gtri.gatech.edu
GTRI Lead CSRs

Revisions and Updates

January 2020
- Updated the name of the GTRI training management system (Quest LMS instead of StarTrak)

October 2019
- Updated purpose to clarify scope of the Master TCP and identify situations that require approval by the Office of Research Integrity Assurance
- Identified approved GTRI locations to use under the GTRI Master TCP
- Updated information security to reference GTRI policies
- Moved institutional commitment to first section
- Added section on "Authorization for Exports"
- General editing throughout the document to improve clarity

January 2019
- Updated procedures for using email during international travel
- Clarified policy for checking email while abroad
- Updated training requirements to register through StarTrak

May 2018
- Updated informational link for travel
- Corrected link to international travel security tips

November 2017
- Updated international travel policies concerning email and use of exemptions
- General editing throughout the document to improve clarity

March 2017
- Revised training requirements to clarify annual training class offered by ORIA

January 2017
- Added requirement to use two-factor authentication

TABLE OF CONTENTS

I. Institutional Commitment 4

II. PURPOSE 4

III. APPLICABLE REGULATIONS & Definitions 5

IV. SCOPE and APPROACH 6

V. INFORMATION SECURITY PLAN 7

VI. PHYSICAL SECURITY PLAN 7

VII. Authorization for Exports 8

VIII. INTERNATIONAL TRAVEL 9

IX. PERSONNEL TRAINING AND AWARENESS 9

X. SELF EVALUATION AND MANAGEMENT SYSTEM 10

XI. Attachment A: Acknowledgement of GTRI Master Technology Control Plan for Export Controlled Information 11

I. INSTITUTIONAL COMMITMENT

It is the policy of Georgia Institute of Technology (GIT) to fully comply with all applicable federal statutes, executive orders, regulations, and contractual requirements for the safeguarding of controlled technical information in its possession. This includes full and total compliance with export control regulations. Under no circumstances shall employees or other persons acting on behalf of GIT engage in activities in contravention of U.S. export control laws. Employees found to be in violation of these directives or the provisions of this plan may be subject to disciplinary actions, up to and including termination of employment. Such violations can also earn civil and/or criminal penalties for GIT and/or the individual making the disclosure.

The intent of this TCP is to demonstrate the appropriate level of security for controlled technologies as it pertains to export control requirements.

It is unlawful under the export regulations to send or take export controlled information and items out of the U.S.; or to disclose such information, orally or visually, or to transfer export controlled information and items to a Non-U.S. person inside or outside the U.S. without proper authorization. A license or other approval may be required for Non-U.S. persons to access export controlled information.

II. PURPOSE

The purpose of this "Master" Technology Control Plan (TCP) is to establish the required controls for the protection of Export Controlled (EC) information and items being utilized during the performance of Georgia Tech Research Institute (GTRI) projects or retained at GTRI.

This Master TCP shall be used for controlling export controlled projects for GTRI personnel in GTRI facilities. An additional project specific TCP may be required to safeguard items outside of GTRI facilities, including Georgia Tech academic facilities.

This Master TCP shall be followed to safeguard all export controlled information to prohibit unauthorized access by foreign nationals and other non-authorized individuals.

The Project Director (PD) must notify the Office of Research Integrity Assurance (ORIA) in any of the following circumstances for any project subject to this TCP.

a) Projects that allow access to technical information by non-US Persons;

b) Projects that will export any export controlled items (including information or data) or provide services outside of the U.S. or to foreign persons

    a. International travel – even if done with federal sponsors or not providing technical information
    b. International shipping

c) Projects that will allow students (including US citizens) to use project information or data to complete a thesis or dissertation;

d) Academic interaction activities that involve collaborative efforts with academic facilities or labs;

Important Note: Projects that will export or share any export controlled information, technology, data, equipment or materials or services outside the USA – even to a US Military installation abroad – may require a license or other approval. Please contact Export Office for licensing or other approvals prior to shipment or release of information. Plan ahead as some licenses or other approvals may require a significant lead time.

In these situations, ORIA will review applicable regulations that may prohibit access by foreign nationals. This includes any projects ineligible for fundamental research or involving export controlled items. ORIA may draft a project specific TCP to outline the appropriate safeguards to prohibit unauthorized access and identify any required licenses or other approvals needed for exports.
This TCP provides a roadmap for how GTRI will control these data, information or materials to ensure that unclassified export controlled information is not provided to Non-US persons (employees, students, colleagues or visitors) without the

required export license from the Department of State and approval from the Offices of Research Integrity Assurance (ORIA) Export Team and Legal Affairs. Additionally, this TCP ensures that all individuals working on a project containing export controlled information understand their obligations under the export control laws and regulations. Disclosures of export controlled information to Non-US persons (whether he/she is an employee, consultant, sponsor, student, or visitor) is considered an export under the export control regulations and requires a license or other approval from the Department of State. Disclosures without the proper authorization can result in fines and jail time *for the individual* making the disclosure.

For contracts or projects that involve an OPSEC Plan/Concept of Operations (CONOPS), the Government or organizational protection/procedural guidelines (i.e., OPSEC Plans/CONOPS) that enhance the TCP requirements will be followed as directed by Research Security.

Please note: Non-US Persons may not be eligible to work on projects that do not qualify for the Fundamental Research Exclusion (FRE) without written approval from the Export Team/ORIA and, when required, a license from the federal government. Additionally, students (including U.S. persons) should not work on any project ineligible for the Fundamental Research Exclusion for their theses or dissertations. If a Non-US person or a student working on a thesis or dissertation is required for this project please contact the ORIA Export desk for assistance with obtaining appropriate approvals and preparing an individual TCP.

III. APPLICABLE REGULATIONS & DEFINITIONS

Further information on these regulations may be found on the Office of Research Integrity Assurance website at https://researchintegrity.gatech.edu/about-export/export_overview

NISPOM – National Industrial Security Program Operating Manual controls the authorized disclosure of *classified information* released by U.S. Government Executive Branch Departments and Agencies to their contractors (DoD 5220.22-M)

EAR – Export Administration Regulations control certain dual-use technologies, materials, items, software and technology through the Department of Commerce (15CFR §§ 730-774)

ITAR – International Traffic and Arms Regulations control the export of defense articles, performance of defense services, including the release of defense article-related technical data through the Department of State (22 CFR §§ 120-130)

OFAC – Office of Foreign Assets Control regulates travel and business activities with sanctioned and embargoed countries from the Department of Treasury

US Person means a person (as defined in § 120.14 of this part) who is a lawful permanent resident as defined by 8 U.S.C. § 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. § 1324b(a)(3) . It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state or local) entity. It does not include any foreign person as defined in § 120.16 of this part. (22 C.F.R. § 120.15)

Foreign Person (or Non-US person) means any natural person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. § 1324b(a)(3). It also means 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 United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions). (22 C.F.R. § 120.16)

License means a document bearing the word “license” issued by the Deputy Assistant Secretary of State for Defense Trade Controls, or his authorized designee, that permits the export, temporary import, or brokering of a specific defense article or defense service controlled by the regulations

Other approval means a document issued by the Deputy Assistant Secretary of State for Defense Trade Controls, or his authorized designee, that approves an activity regulated by the regulations (e.g., approvals for brokering activities or retransfer authorizations), or the use of an exemption to the license requirements as described in the regulations.

In general, an **export** of controlled information refers to the transfer/disclosure of items, materials, information, software, technology or other unclassified but restricted data to any person outside U.S. (including U.S. citizens abroad) or to any foreign person (deemed export) inside the U.S. 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.

Items may include materials, equipment, software, data, information or technology

Fundamental research

IV. SCOPE AND APPROACH

The Project Director for each project is responsible for compliance with this TCP. Additionally, all GTRI personnel producing or accessing export-controlled information or items and will include all operating locations, offices, temporary operating locations, and facilities whether located on campus or during visits to military reservations or in Government office buildings. Employees shall ensure compliance with the spirit and intent of the protection criteria contained herein and will be especially cautious when dealing with Non-US persons or entities, whether within the United States or abroad. This TCP has been put in place to ensure that transfers of export controlled items to Non-US persons does not occur without appropriate authorization. Each project will require adherence to 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.

This plan is required because one or more of the following conditions exist:

Export Controlled under a Classified Project:
This project may involve classified information/equipment which, in itself, is export controlled. Handling of classified information is delineated in the NISPOM and this TCP does not modify the handling requirements for classified information. No release of classified information (i.e. confidential, secret, top secret) is permitted to any person without the proper security level clearance and a documented "need to know" for that specific information. The purpose of this TCP is to define the controls necessary for handling the unclassified but still export controlled items, materials, equipment, software, data, information or technology.

Export Controlled under an Unclassified project:
This project may involve access to unclassified export controlled items. Access to export controlled items may be indicated in a sponsored agreement, statement of work, confidentiality or non-disclosure agreements, data use agreements, and teaming agreements.

Publication or Foreign National Restriction:
Agreements that include publication or foreign national restrictions are not fundamental research and therefore all research results are *subject* to export control regulations. Access by foreign nationals is prohibited and all requirements of this TCP must be followed unless written approval has been received from the Office of Research Integrity Assurance. Approval may be also require sponsor approval. Access by foreign nationals will consider export regulations, including the need for an authorization or other approval, along with considerations for nationals security. The Project Director and project participants may not release any information or publish results of the research without the prior approval unless the information or research results have already been placed (legally) in the public domain.

Any technology that is controlled under ITAR, will require an authorization or other approval from the Department of State to allow access by Non-US persons. The Project Director and all employees who have supervisory responsibility of non-US persons will be fully aware of their responsibilities regarding possible technology transfer and access control issues. In the event the project involves Non-US persons, contact the ORIA Export Team for assistance with preparing an export authorization or other approval.

NON-US PERSON VISITS OR CO-LOCATION OF NON-US PERSONS

To ensure compliance with federal regulations and protect GTRI research participants from unintentional disclosures, controls must be in place to prevent unauthorized access to non-US persons. Non-US persons, including collaborators, visitors or tours, may not have access to GTRI facilities where export controlled research is conducted, including but not

limited to research project data, information, materials, etc. without prior written approval from the ORIA Export Desk, an institute Empowered Official, and proper authorizations when required. A TCP or Technology Monitoring Plan (TMP) may be put in place to address the possible risk of an unintentional disclosure for any non-US Person or tour of the facility.

From time to time it is appropriate to co-locate a non-US Person within GTRI space or facilities due to research or programmatic needs. Prior to placement of any non-US person (paid or unpaid, employee or visiting scholar or guest) within GTRI facilities where export controlled research is conducted, an export review must be conducted to determine if any additional precautions or authorizations are required. It is the responsibility of the Lab Director to contact the Export Desk at export@gatech.edu for prior written approval and when appropriate, an individual TMP for the non-US person or licenses if required.

GTRI personnel that find themselves working with or co-located with a non-US person are personally responsible for verifying that an export review has been conducted and the non-US person has been approved for the project and work location. GTRI personnel may contact their Lab Director or the Export Desk to verify Export review and approval for the non-US person. Any export controlled technical data, information, materials, etc. that are shared or provided to a non-US person without a license or exemption could result in an unlawful export requiring a Voluntary Self Disclosure.

V. INFORMATION SECURITY PLAN

Export controlled information may not be posted on networks with uncontrolled shared access. All GTRI policies (https://webwise.gtri.gatech.edu/inside-gtri/policies/gtri-policies-procedures), including, but not limited to 8000 Information Technology, must be followed closely to prohibit access by non-authorized persons and all foreign nationals.

Data Storage

In particular, closely review the GTRI options to store and share data. This includes the use of cloud providers contracted by GTRI. The matrix outlining the resources is available in the Information Systems (ISD) “How To’s And Instructions” (https://webwise.gtri.gatech.edu/information-systems-department/how-tos-and-instructions)

VI. PHYSICAL SECURITY PLAN

Buildings and work areas within GIT including GTRI Field Offices involved in classified work are protected in accordance with the guidelines of the NISPOM incorporating such protective measures as card reader access, Non-US person escort requirements, spin dial door combination locks, video monitoring, and guard force presence as required by RSD. Unclassified export controlled information will be protected, at a minimum, in accordance with the guidelines of this TCP.

The physical security of export controlled equipment and data will be ensured and shall be shielded from unauthorized persons. Non-US persons shall not have access to export controlled equipment or data without authorization by a valid authorization or other approval as needed..

GTRI Facilities include: List updated October 2019 from https://gtri.gatech.edu/locations

Export controlled technical information, data, materials, software, or hardware, *i.e.*; technology generated from this project, must be secured from use and observation by unlicensed Non-US persons by being secured in a locked desk drawer, locked filing cabinet, or locked office. Security measures will be appropriate to the sensitivity involved. Non-US persons will be provided a segregated enclosed workspace and will be escorted or monitored by an authorized employee. Project Directors who have supervisory responsibility for non-US persons must receive an export control briefing that addresses relevant ITAR requirements as they pertain to export controlled information.

Conversations and Discussions

Conversations and discussions about the project or work products are limited to US Persons as defined in the US export regulations. Conversations and discussions shall be held only in areas where unauthorized personnel are not present. Conversations and discussions may not take place in public locations where non-US persons are present.

Presentations

Persons presenting research findings or other technical information at open conferences may not divulge information subject to export control regulations without prior approval of DDTC or BIS. Sponsored project agreements containing export controlled items, materials, equipment, software, data, information or technology may require that project personnel

obtain written sponsor approval before the release of a publication or presentation. These requests shall be made in compliance with, and within the time frame stated in the sponsored project agreement. If no time frame is stated in the project agreement, three to six months may need to be anticipated for approval to be received from the contracting officer. Public release of information shall not occur until any required permission or other government approval is received by U.S. Department of State, Directorate of Defense Trade Controls, (DDTC), or U.S. Department of Commerce, Bureau of Industry and Security (BIS).

Publication
In most cases, restricted research will contractually require that project personnel not release or disseminate any information pertaining to the project without the prior written approval of the sponsor, excluding information already in the public domain. In situations that there is not a contractual publication restriction (such as IRADs) and the project involves controlled items, research results and publications generated from the controlled items may still be subject to the regulations.

Generally, when projects that are subject to the approval of the sponsor, the impact of such restrictions should be considered prior to employing graduate students and tenure track faculty. Publications (including but not limited to theses, dissertations or journal publications) may be delayed or denied based on the approval of the sponsor or US government.

Marking of Unclassified Export Controlled Information
The appropriate markings for export controlled information may be determined by the sponsor (e.g., CUI or DOD Distribution Statements). In the absence of these requirements, technical documents that are determined to contain export-controlled technical data shall be marked in a manner to notify others who receive the document. Possible marking is "WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25." When it is technically not feasible to use the entire statement, an abbreviated marking may be used. If applicable, designated publication distribution statements shall be placed on the material.

Disposal
All items will be destroyed using appropriate sponsor approved measures. In the absence of sponsor direction, all physical items will be shredded, torn, or dismantled such that the controlled technology information contained within is indistinguishable. Files on hard drives will be deleted using appropriate measures. GTRI RSD destruction resources shall be used for properly disposing of controlled information and/or equipment located in the Atlanta area. GTRI Field Offices can also utilize this method of destruction if necessary.

Freedom of Information Act (FOIA) and GA Open Records Act (ORA)
As a public educational institution of the State of Georgia, GIT has certain obligations to respond to requests for "public" information. The Freedom of Information Act and applies to requests for information made to federal agencies and thus, GIT is not subject to FOIA. The state equivalent of the Federal act is the GA Open Records Act (ORA). The ORA provides all citizens an opportunity to request the records of state agencies and to make copies for a fee. The ORA requires that Georgia Tech produce public documents within three business days. If you receive a request for records under either Act, please contact the GT OLA immediately.
Not all Institute information is subject to state statutes, and each request for information is reviewed by appropriate administrators and the GIT OLA for our legal obligations for release or protection of the information.

VII. AUTHORIZATION FOR EXPORTS

Physical Mail
Export controlled documents and material may be transmitted via first-class mail, parcel post or fourth-class mail (for bulk shipments). All international shipments on sponsored research projects must be approved by the ORIA Export Desk or the OLA. Biological and chemical shipments must be taken to Environmental Health and Safety (EH&S) for packing and shipping.

The following Destination Control Statement should be included by on international shipments:
"These commodities, technology or software were exported from the United States in accordance with the EAR or the ITAR. Diversion contrary to U.S. law is prohibited."

VIII. INTERNATIONAL TRAVEL

Individuals may not take or work on export controlled projects/information when traveling abroad without prior authorization. Export controlled items should only be taken abroad when required for the conduct of the project.

a) Laptops, tablets, phones (including Blackberries, iPhones, smartphones, etc.) containing export controlled information may not be taken even if controlled information is encrypted or not accessed. In order to minimize the risk of unlicensed data export, the following options are recommended:
   i) Only take "clean" electronic devices (e.g., laptops, tablets, phones). These devices must not contain any unlicensed export controlled information, should be encrypted, and should only contain user data necessary for the trip. GTRI can provide loaner electronic devices for international travelers including computers and smartphones.
   ii) All devices (excluding GTRI-loaner devices) should be reviewed prior to departure to ensure compliance with export control laws including encryption regulations (submit to OLA via TAR prior to travel).
   iii) Retain physical possession of all electronic devices while outside of the U.S.

b) If you need to check GTRI email while out of the country and you normally receive export controlled emails in your inbox, you must proceed carefully.
   i) If you are travelling to a non-126.1 country, GTRI email may be checked under the following conditions:
      (1) You should purge your email folders of all ITAR before you leave. In general it is a good practice to not store ITAR and sensitive data in your email folders long term.
      (2) You should only use the web interface to read your email. You can log on through https://mail.gtri.gatech.edu
      (3) If you do receive an email that you believe may contain ITAR, you should delete it and not open the email. If you do this, no report is necessary.
      (4) If you do accidentally open an email containing ITAR (thus downloading it in a foreign country), you must report this to Mary Beran in GTRC. Since you are not in a 126.1 country, it is not a major violation, but needs to be reported and logged.
      (5) Only use secure devices to check your email via the web
         (a) "Clean" loaned from GTRI that has adequate encryption installed
         (b) GTRI mobile device with AirWatch installed. Do not use either the native mail client or Boxer to read email on your mobile device as that would download/export any potential ITAR document.
   ii) If you are travelling to a 126.1 country (https://bit.ly/2CfmpDD), a travel email must be used. A CSR will set up a second account such as JohnDoe_In_China@GTRI.gatech.edu for you and put an out of office message in your normal account saying that Non-Export Controlled emails can be sent to the outside-the-USA address (JohnDoe_In_China@GTRI.gatech.edu). If you do retain and use your regular GTRI email address while on travel and receive export controlled information delete it immediately and inform RSD and Export as soon as practical.

More information can be found at: https://security.gatech.edu/traveltips.

IX. PERSONNEL TRAINING AND AWARENESS

All GTRI personnel who potentially have access to Export Controlled data/information/materials or are responsible for the administration of export controlled activities (such as financial managers, coordinators) are required to attend annual training. If you are unsure if you should attend, discuss with your manager and the Office of Research Integrity Assurance.

Training designed for the needs of the GTRI community is available at various GTRI Locations, including GTRI Headquarters (GTRI Conference Center - 14th Street) and GTRI Cobb County Research Facility (CCRF). GTRI Personnel can register for training through the Quest LMS system used for other GTRI training opportunities.

Personnel located at field offices outside of the Atlanta area may attend remotely via the web. Register for a GTRI session in Quest LMS, then contact the GTRI Training team at gtritrainin.ask@gtri.gatech.edu for connection information. Personnel in the Atlanta area (including CCRF) are expected to attend in-person.

All project personnel must read and understand this TCP, sign Attachment A, and attend Export Control Training to work on the project or be charged to it. Project personnel must be aware of their responsibilities to prevent inadvertent or other inappropriate disclosure of controlled items and of the personal criminal and civil penalties (including prison sentences of

up to 10 years and fines of up to $1M) for failure to comply with U.S. export control rules. All project personnel will be screened against the applicable restricted parties' lists. The Project Director is responsible for ensuring all new project participants have reviewed the TCP and attended training before allowing access to project items, materials, equipment, software, data, information or technology.

X. SELF EVALUATION AND MANAGEMENT SYSTEM

A thorough review of this TCP will be conducted by the ORIA, OLA and RSD on an annual basis to ensure compliance with federal security requirements and to determine whether changes, updating, or upgrading of the TCP protective measures are warranted. Each GTRI Director will also initiate a periodic internal review of this TCP to ensure that the compliance system is operating effectively. If changes are required, the PI will forward proposed changes to ORIA and RSD for review and approval. The annual and periodic review will include a check of the project personnel listing, random personnel interviews, verification of physical security protective measures, and a review of the information security protective measures. A project specific TCP will be drafted if this TCP is unable to fully protect the information for the project.

REPORTING AND RESPONSIBILITIES

Any person having knowledge of a potential violation or noncompliance with the provisions of this plan or any applicable export control directive shall immediately report the circumstances surrounding the activity to the ORIA Export Desk and GTRI RSD. The reporting can be accomplished via the below listed points of contact. When appropriate, GIT shall disclose involvement in violations to the proper authorities in accordance with applicable regulations. Any deviation or waiver from or exception to these procedures requires prior approval of the signatories hereto. Any violation of the terms of this plan may be grounds for disciplinary action. Business managers must read the TCP and agree not to process a PSF to add non-US person personnel to applicable projects without the prior approval from the ORIA Export Desk.

All project participants must report any suspicious or unsolicited request for export controlled information by unauthorized persons. Unsolicited contacts can be in the form of email, personal or telephonic questioning. Unsolicited emails will be forwarded to suspicious.email@gtri.gatech.edu. Personal or telephonic queries can be reported through email descriptions of the query and unauthorized person involved. Regardless of whether the contacts seem suspicious they should be reported immediately.

reportacontact@gatech.edu should be used by all GT personnel in the Study Abroad, Work Abroad programs or Traveling Abroad.

CONTACT INFORMATION

Primary Point of Contacts: Email all correspondences regarding export concerns to export@gatech.edu

Export Control:
Mary M. Beran, MA, CPIA
Director & Empowered Official
Office of Research Integrity
Office: 404.385.2083
Cell: 404.290.2160
mary.beran@gtrc.gatech.edu

Export Control:
Rhonda Shaner, M.Ed.
Research Associate
Office of Research Integrity
Office: 404.385.0288
Cell: 404.654.2910
rhonda.shaner@gtrc.gatech.edu

Research Security:
Dannie K. Lyvers Jr.
Insider Threat Program Senior Official (ITPSO)
Research Security
Georgia Institute of Technology
(404) 407-7442 (Phone)
(404) 293-6682 (Mobile)
dannie.lyvers@gtri.gatech.edu

Export Website: http://www.export.gatech.edu/export-control

XI. ATTACHMENT A: ACKNOWLEDGEMENT OF GTRI MASTER TECHNOLOGY CONTROL PLAN FOR EXPORT CONTROLLED INFORMATION

Acknowledgement of Technology Control Plan and Non-Disclosure Statement

I hereby certify that I have received, read, and understand the GTRI Master TCP for handling Export Controlled Information and the procedures contained in this TCP. I agree to comply with the restrictions contained herein and with U.S. Government regulations as they pertain to 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 understand that I must attend export control training before working on any export controlled projects and that I must complete annual training thereafter.

I hereby acknowledge and understand that any information related to defense articles restricted by the Department of State under the ITAR on the U.S. Munitions List or articles restricted by the Department of Commerce under the EAR (, to which I have access or which is disclosed to me in the course of my (employment-assignment-enrollment-visit) at Georgia Institute of Technology, is subject to export control under the ITAR or the EAR. I hereby certify that such data will not be further disclosed, exported or transferred in any manner to any non-US person or entity without prior written approval of the Office of Research Integrity Assurance and required authorization or other approvals from federal agencies, if required. If I inadvertently export to an unauthorized recipient any controlled items, materials, equipment, software, data, information or technology received during my employment-visit-enrollment, I will report such unauthorized transfer promptly to the ORIA Export Desk and acknowledge the transfer to be a violation of U.S. Government regulations.

Print/Type Name: _____ Date: _____

GTRI Unit: _____

GIT/Kerberos ID: _____

☐ US Citizen (if more than one citizenship please list all citizenships below)

☐ US Person (under export regulations): Permanent Resident (Green Card holder)
Country of citizenship(s) (list all if multiple citizenships):
_____

Please note: Non-US Persons may not be included under the GTRI Master TCP. Additionally, students (including U.S. persons) may not work on any project ineligible for the Fundamental Research Exclusion for their theses or dissertations (student hourly work is allowable). If student involvement will be used for their thesis/dissertation, please contact the ORIA Export desk for prior approval.

Signature: _____

Return Signed Attachment A to:
Dannie Lyvers, GTRI RSD dannie.lyvers@gtri.gatech.edu
CC to Export@gatech.edu.