

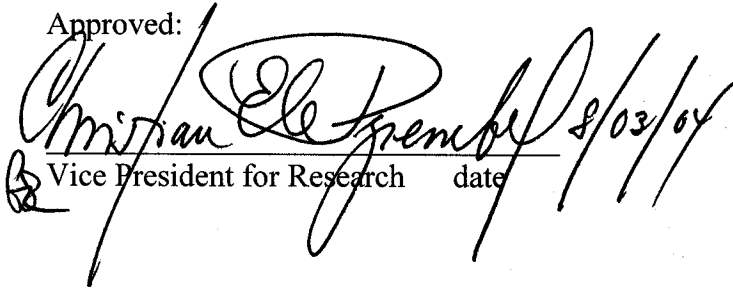
# Clemson University

## Technology Control Plan

Modification 2

8/02/2004

Approved:

 Christian El Greco 8/03/04  
Vice President for Research      date

Federal Controlling Agency:  
U.S. Defense Security Service  
Charleston AFB, S.C.

*hshare:export control;TCPrevisioncopy\_mod2\_08022004*

## **Clemson University Technology Control Plan**

### **I. Overview**

As a public institution of higher education, Clemson University (CU) employs individuals of foreign nationalities and often hosts foreign visitors in connection with international exchange programs, international students, and other business agreements. It is the intent of CU to employ foreign nationals and host international visitors, both long and short term, in the most welcoming manner possible while also assuring compliance with U. S. laws and regulations governing the export of certain commodities and technical data.

The U.S. Department of Commerce regulates certain dual-use technologies, materials, and items by the Export Administration Regulations (EAR) and the U.S. Department of State controls the export of defense articles, defense services and defense-related technical data through the International Traffic in Arms Regulation (ITAR).

Each employee is personally responsible for safeguarding export-controlled data/information, i.e. Controlled Technical Data, as required by the above federal agencies from disclosure to foreign persons without prior approval. An export license from the U.S. government is required before a foreign national may be given access to hardware or technology controlled by either the U. S. Department of Commerce or the U. S. Department of State. 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.

Persons presenting research findings or other technical information at open conferences may not divulge information subject to export control regulations. Sponsored agreements associated with containing export control technology or materials require project personnel to formally request and obtain prior approval before the release of a publication or presentation. These requests shall be made in writing to the sponsor’s contracting officer or to the individual identified by the sponsor, and must be within the time frame stated in the 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 permission is received by U.S. Department of State, Office of Defense Trade Controls, (ODTC), or U.S. Department of Commerce, Bureau of Industry and Security (BIS). Such requests and responses to those requests for authorization and/or coordination shall be submitted through the University’s Technical Control Plan Officer assigned within the Research Compliance Office.

### **II. Purpose**

The purpose of this Technology Control Plan (TCP) is to delineate the controls necessary to ensure that the transfer of technical and/or classified information data is not conveyed in any manner to foreign national visitors, employees, and students beyond that which is approved for export by a formal license from the appropriate U.S. federal agency, or which is authorized to an individual possessing the required security classification and “need to know.”.

### **III. Existing Policies and Procedures CU**

Regarding the handling of classified information reference is made to Clemson University’s agreement with the U. S. Department of Defense document dated March 3, 1982. This agreement requires CU’s adherence to the National Industrial Security Program Operating Manual. These documents shall be considered a part of this TCP, by reference.

#### **IV. Definitions**

##### *A. Controlled Technical Data*

Controlled technical data, (which includes materials and equipment) are defined as follows:

1. Information (i.e. technology), other than software as defined below, material and equipment which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles or included in the U.S. Munitions Lists (USML). Information may be in the form of blueprints, drawings, photographs, plans, instructions, and documentation. Information, material or equipment falling within the above categories also includes that which is still in the “working” or “developmental” stage, regardless of “in process” or “deliverable” status. The release of such information, materials, and equipment via any means (e.g. shipping) or media (e.g. spoken, or written) is not permitted without prime sponsor approval.
2. U.S. Government classified information relating to defense articles and defense services; classified information shall include all documents/information marked by any U.S. federal agency as NoFORN (No Foreign Dissemination), Confidential, Secret and Top Secret.
3. Information covered by an invention secrecy order;
4. Software, as defined below, directly related to defense articles;

Controlled Technical Data does not include information or software concerning general scientific, mathematical or engineering principles currently in the public domain. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles. ITAR (22 CFR 120 - 130) (reference c) NOTE: For security assistance and government contracting purposes, the Security Assistance Management Manual (SAMM para 140104.B) and the DEARS (Section 227.401(18) define "technical data" differently.

Disclosure of unclassified technical data controlled by the International Traffic in Arms Regulations (ITAR) to foreign nationals in the course of employment with U.S. contractors is considered an export disclosure and is subject to and requires a U.S. government export license prior to disclosure. Administration of the ITAR is conducted by the Office of Defense Trade Controls (ODTC), Center for Defense Trade, Department of State.

For general application of this TCP the terms “technical data”, “materials”, or “equipment” are interchangeable in the context of what must be controlled. An unauthorized release to a foreign national can result in severe civil and criminal penalties imposed upon the offending individual. Individuals must be careful that an unauthorized “release” or transfer action does not inadvertently occur during meetings, telephone conversations, facilities visits, or other circumstances.

##### *B. Technical Information (Technology)*

Information, i.e.. technology, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment. (DoD Directive 5200.21).

##### *C. Foreign National*

The ITAR defines a “foreign national” as any person who is not a citizen or national of the U.S. unless that person has been lawfully admitted for permanent residence, (i.e., is under immigrant-visa status, or individuals referred to as "immigrant aliens" under previous laws), in the U.S. under the Immigration and Naturalization Act (8 U.S.C 1101, section 101 (a) 20, 60 State. 163). The definition includes foreign corporations, i.e., corporations that are not incorporated in the U.S., international organizations, foreign governments and any agency or subdivision of foreign governments (e.g. diplomatic missions).

The National Industrial Security Program Operating Manual (1995 version) distinguishes between a "foreign national" and an "immigrant alien," the latter defined as "any person lawfully admitted into the U.S. under an immigration visa for permanent residence" (i.e. one who possesses permanent resident, or immigrant-visa status). **Foreign students that are on non-immigrant status are therefore considered foreign nationals.**

*D. Export*

The ITAR (22 CFR 120-130) (reference c) defines "export" as:

1. *Sending or taking a defense article out of the U.S. in any manner, except by mere travel outside the U.S. by a person whose personal knowledge includes technical data; or*
2. *Transferring registration or control to a foreign person of any aircraft, vessel, or satellite covered by the US. Munitions List, whether in the U.S. or abroad; or*
3. *Disclosing (**including oral or visual disclosure**) or transferring in the U.S. any defense article to an embassy, any agency or subdivision of a foreign government (e.g. diplomatic mission); or*
4. *Disclosing (**including oral or visual disclosure**) or transferring controlled technical data to a foreign person, whether in the U.S. or abroad; or*
5. *Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the U.S. or abroad.*

**In summary, an "export" occurs whenever controlled technical data, materials, or equipment is disclosed in the U.S., or abroad, to a foreign person. If an export of technology, i.e. information, occurs within the U.S., that action is termed a "deemed" export.**

*E. Software*

Software includes, but is not limited to, the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair.

*F. Public Domain*

All information that is currently published, generally accessible, or available to the public. For example:

1. Through sales at news stands and bookstores;
2. Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information; or
3. At libraries open to the public or from which the public can obtain documents;
4. Through issued patents;
5. Research in science and engineering at accredited institutions of higher learning where the resulting information can be published and shared broadly within the scientific community. Such research is termed "fundamental research" and is not subject to security classification or export control procedures. However, sponsored research conducted by a university is not considered "fundamental" if:
  - a. The University or its researchers accept sponsor's restrictions on publication of scientific and technical information resulting from the project if the sponsor has indicated such action is required as a result of U.S. classified or export license control procedures; or,
  - b. The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable, e.g., ITAR (22 CFR 120-130).

### G. *Proprietary Information*

Information belonging to CU or provided to CU by another party which is identified in writing as "confidential" or "proprietary" and that:

1. Is not generally known or in the public domain,
2. Was not in a party's possession or was not known to it prior to its receipt from a disclosing party under a nondisclosure agreement,
3. Is not available on an unrestricted basis to a third party from the disclosing party or from someone acting under its control,
4. Is not required to be released by a court of competent jurisdiction, or otherwise required by law.

### H. *Defense Articles/Services*

For the purpose of the TCP, such articles and/or services are those controlled under either the Arms Export Control Act (AECA), Pub. L. 94-329 (1976), (22 USC 2751) for national defense, or the Export Administration Act of 1979, (EAA), Pub. L. 96-72, (50 USC 2401-2420) as amended for dual use, non-military applications. The term "defense article" under 22 CFR 120.6 is defined to include both "items" and technical data.

## V. **Scope**

CU is an educational institution with its mission being education, research, and public service. In the course of fulfilling its mission, CU hosts, educates, and employs foreign nationals.

Except to protect a sponsor's proprietary information, or for brief delays to undertake patent application processes, when the University allows the sponsor to place a restriction, e.g., prior approval on the publication, or dissemination of the results of a project, export control requirements must be implemented. Only by maintaining its right to control the dissemination of the findings of a project is the University able to obtain exemption from export control regulations as provided to it under the claim of "fundamental" research (reference IV, F, 5).

This plan delineates the procedures established to ensure that no transfer of controlled technical data occurs beyond that which is approved, i.e. a license to export has been granted, by the ODTC and the Department of Commerce.

## VI. **Procedures Governing Access to Controlled Technical Data, Materials, Items**

### A. *Foreign Nationals Procedure*

Foreign nationals, whether they be students, visitors, conference participants, etc., or employees of the University, may not have access, in any capacity, to controlled technical data unless license authority has been granted by ODTC, the Department of Commerce or other authorized federal agency, e.g. DOE. Provisos and limitations included in the approval must be implemented prior to the transfer of any export of data, materials, etc. subject to export control.

### B. *Access Oversight*

The Office for Sponsored Programs (OSP) will notify principal investigators of funded projects of their responsibility to the sponsor and the University for the observance of this TCP whenever they receive a contract involving classified or controlled technical data. This will be accomplished by appropriate notice with supporting documentation such as memoranda, a copy of the TCP, and a briefing of the principal investigator and execution of Attachment A, Technology Control Plan Briefing. The principal investigator who has supervisory responsibility of any foreign national will be briefed in those areas of export control as set forth in this TCP. In addition, copies of this TCP will be issued to the principal investigator's immediate Director or Department Chair. The principal investigator assumes the responsibility to provide a copy of the TCP to appropriate project personnel in order to

obtain their signature on Attachment A, Technology Control Plan Briefing prior to their participation in the project. Copies of the signed attachment is forwarded to the TCP administrative office.

Prior to submission of a proposal in which the principal investigator desires to have a determination as to whether an award would cause the TCP to be imposed upon the project's performance, contact with the Office for Sponsored Programs is recommended.

C. U.S. Government Classified Technical Data, Material, Items (e.g., contracts that incorporate FAR Clause "Security Requirements, 52.204-2, or DEARS 952.204-2)

Information is releasable only to those individuals (e.g. employees, graduate students, visitors, etc.) with the appropriate U.S. security clearance (confidential, secret, top secret, etc.) and the appropriate need-to-know, as determined by the possessor of the classified information. The handling of classified information is discussed in detail with the principal investigator and the University's Facility Security Officer. Classified information is not authorized for release or disclosure to any foreign national. No classified access will be provided to the foreign national, thereby prohibiting access to facilities, documentation, and records, as well as prohibiting foreign nationals access to design, development, and test areas where classified work is in process.

Foreign nationals will not be authorized access to classified contracts without proper authority.

D. Unclassified Controlled Technical Data, Materials, Equipment

Federal or private industry agreements which contain a specific national security control measure (e.g., right to withhold publications, restriction on participation of non-US citizens, etc) or which otherwise contractually subjects the project activity to export control procedures should be cared for by project personnel as described by the examples listed in Attachment C, "Guidelines for the Protective Security of Technical Information, Data, Materials, and Equipment."

Foreign nationals can not be granted access to controlled technical data without formal approval (i.e., an export license) from BIS or ODTC as appropriate. The individual desiring to transfer controlled technical data, materials, or equipment to a foreign national is responsible for obtaining the appropriate approval through the formal channels established by those federal agencies.

Access to controlled data or materials granted to U.S. citizens should be preceded by written notification of the controlled nature of the data or materials to the recipient with copy retained by the provider.

If the publication, or any disclosure of the project's findings is subject to review and prior approval by contracting officer, once that approval is received, the information contained in that disclosure can, therefore be placed in the "public domain" and, consequently, is no longer considered export controlled.

E. Proprietary Information

1. CU Proprietary Information

CU proprietary information is protected internally by confidential invention disclosures and internal nondisclosure agreements as may be necessary. Release of CU proprietary information externally occurs only after a nondisclosure agreement is executed between the party releasing and the party receiving the information.

2. Proprietary Information Received by CU

This information is protected under the terms of each individual nondisclosure agreement as may be negotiated and executed by the parties involved unless the information is required to be released by a court of competent jurisdiction or as otherwise required under legal proceedings.

## **VII. Foreign Nationals**

Academic departments will be responsible for appropriate orientation of all new employees, graduate and undergraduate students, including foreign nationals employed by their departments for projects that fall within this Technology Control Plan. When appropriate, all foreign nationals will be briefed and/or informed concerning those areas of export control and export licensing actions that are pertinent to their activities.

After receipt of an export license, the foreign national to whom controlled technical data will be disclosed shall sign the Nondisclosure Agreement (Attachment B), a copy of which will be subsequently forwarded to the TCP administration office noting the assigned license number.

## **VIII. Administration**

Administration of the TCP is the responsibility of the University's Technical Control Plan Officer, assigned to the Research Compliance Office, as it applies to the release of controlled technical data of U.S. origin in a foreign country or to a foreign entity. Clemson University's Technical Control Plan Officer will request a counter intelligence briefing visit from the Defense Security Service on an annual basis.

Principal Investigators and/or department heads are responsible for ensuring that employees in their activities are properly instructed in the handling of classified, export-controlled, or proprietary information and that they have signed the required briefing document, Attachment A prior to involvement in the project.

Clemson University's Technology Control Plan (TCP) Officer:  
Director, Office of Research Compliance

Other University management personnel supporting the TCP's implementation and administration:  
Director, Office for Sponsored Programs

## **IX. Summary**

As a public educational institution of the State of South Carolina, CU has certain obligations to respond to requests for "public" information. However, not all information of the University is subject to state statutes and each request for information is reviewed by appropriate administrators/University Counsel for our legal obligations for release or protection of the information. CU believes sufficient control and supervision will exist in regard to all employees, undergraduate and graduate students, including those with foreign national status, as regards technology transfer or release of technical know-how. It is the intention of CU to protect all its information not in the public domain unless appropriately authorized by a court of competent jurisdiction, applicable state statute, or the U. S. Government as may be required in each individual case.

In order for Clemson University assume responsibility to meet federal regulations previously cited, no employee, graduate/undergraduate student or other employee or other person acting on behalf of CU shall, disclose, or transmit controlled technical data, as herein defined, without full compliance to this policy document.





**ATTACHMENT B**  
(Revised 5/30/01)

**Foreign National's  
Nondisclosure Statement\***

Project Account:

Sponsor Name & Project Title:

I, \_\_\_\_\_, as a Foreign National, acknowledge and understand that any technical data related to defense articles on the U.S. Munitions List, to which I have access or which is disclosed to me in the course of my association with Clemson University, is subject to export control under international Traffic in Arms Regulations (Title 22, Code of Federal Regulations, Parts 120-130) and/or Export Administration Act (Pub. L. 96-72), (50 USC 2401-2420). I hereby certify that such data will not be further disclosed, exported, or transferred in any manner to any other foreign national or any foreign country without approval of the Office of Munitions Control, U.S. Department of State.

\_\_\_\_\_  
(Signature)                      Date

\_\_\_\_\_  
(Printed Name)

Acknowledgement of Immediate Supervisor:

\_\_\_\_\_  
(Signature)                      Date

\_\_\_\_\_  
(Printed Name)

**\*This statement is to be completed only after a license to export to the named individual has been received from the U.S Department of State or Commerce, as applicable.**

## ATTACHMENT C

### **Guidelines for the Protective Security of Technical Information, Data, Materials, and Equipment**

Program security will be managed according to the guidelines for Export Security. Specifically, technical information, data, materials, software or hardware, i.e., technology, generated from this Subcontract will be secured from use and observation by non-U.S. citizens. Examples of some methods to provide this security are as follows:

- Project Personnel – The use of security badges may be necessary as an aid to identify personnel whose access to project facilities and work-in-progress is authorized.
- Laboratory “work-in-progress” – Project data and/or materials must be physically shielded from observation by unauthorized individual by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.
- 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 – Database access will be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology. Communications via telephone must have similar encryption capability.
- 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 conducted under signed confidentiality agreements that fully respect the Non-U.S. citizen limitations for such disclosures. Execution of Confidentiality Agreements may require formal approval of the federal contracting officer.

Project investigators are cautioned that the publication or other public disclosure, by any means, of technical information, data, materials, or software generated under an export-controlled contract by the University, or Subrecipient may require approval by the Federal Contracting Officer (or sponsor) prior to that disclosure.

Under 22 U.S.C. 2778 the penalty for unlawful export of items or information controlled under the ITAR is up to 2 years imprisonment, or a fine of \$100,000 or both. Under 50 U.S.C., Appendix 2410, the penalty for unlawful export of items or information controlled under the EAR is a fine of up to \$1,000,000, or five times the value of the exports, which ever is greater; or for an individual, imprisonment of up to 10 years, or a fine of up to \$250,000, or both.

Non-U.S. Citizens: Foreign governments, foreign corporations and their representatives, and citizens of such foreign countries.

U. S. Citizens: Includes those individuals whether by birth, or naturalization, and legal aliens with “Green-Card” status, i.e., “permanent resident” aliens.