1.0 Introduction and Background

The University of Wisconsin has a policy of open research. In general, classified projects and any restrictions on freedom to publish are prohibited. UW System General Administrative Policy (GAP 2) states “No agreement shall be entered into with any extramural sponsor which prohibits the right of a University employee to publish the results of the project. The University and its employees have an obligation to assure that project results are made known to the general public.”

A conflict between this policy and a recent change in federal law concerning export control creates an urgent need for SSEC employees to understand the law and how compliance with export laws and regulations can be done consistent with University policy.

Export control regulations arise from the policy of the United States to limit proliferation of weapons of mass destruction and their means of delivery. It is also intended to satisfy treaty obligations of the United States.

Until recently, this issue has not been a problem because an executive order signed by President Reagan freed universities from export control concerns. (see NSDD 189 attached)

But, the 1999 Thurmond Defense Reauthorization Act (excerpts attached) changed how export control was defined and administered. The major changes affecting us were to transfer administration of export control from the Department of Commerce to the State Department where the governing rules are defined in the “International Traffic in Arms Regulations” commonly known as “ITAR.” Part 15 of the ITAR defines spacecraft and associated items as subject to export control.

It is important to understand that the law applies to individuals and the responsibility to comply with the law rests upon each individual. Compliance is not made easier by the fact that the definitions of sensitive items are broad and vague, according to legal experts, and their specific application is subject to wide variations in interpretation. This makes compliance difficult but no less necessary.

The foundation of our export control procedure is built upon the exemptions provided in the export control regulations for items in the public domain, which include fundamental research carried on by universities. It is critical, for both compliance reasons and the University’s continued ability to conduct research, that we minimize contact with items and information subject to export control.

It is also important to understand two concepts: “intangible technology” and “deemed export” because the export control regulations prohibit deemed export of intangible technology. Intangible technology includes information, which may be verbal, electronic, or visual observation by another party. Deemed export can occur in the United States when a non-US person, receives information. (A “US Person” is defined in ITAR as a US
citizen, or permanent resident. ITAR also provides an exemption for Universities so that full-time employees from certain (but not all) countries may be treated as U.S. persons. The clash of the combination of these two concepts with our traditions lies at the heart of our compliance challenge: our work involves matters that can be subject to these controls yet we work in an environment designed to be open to all. And in order for this environment to remain open it must continue to foster free and unfettered communication.

2.0 SSEC Policy for Export Control

This procedure is intended to help SSEC employees and others associated with SSEC projects comply with the export control requirements of the International Traffic in Arms Regulations (ITAR). ITAR prohibits export of items (tangible technology) and information about those items (intangible technology) listed in the regulations. Spacecraft and associated hardware, software, and information are included in part 15 of the list of controlled items.

One very important key to our compliance is that items and information that are in the public domain are not subject to export control. There is a specific provision in ITAR defining “basic and applied research” at “institutions of higher learning” as being in the public domain, which we refer to as the “research exemption”.

The elements in our compliance approach are:

- Rigorously defend our public domain research exemption by maintaining clear records of what this includes and by active and timely publishing.
- Strictly limit contact with information subject to ITAR control so that it does not “contaminate” our fundamental research exemption
- Handle any ITAR sensitive material (items or information) carefully to prevent export.
- Maintain an awareness of the law, the regulations, and how they affect us
- Maintain clear and complete records

The following sections address each of the elements listed above.

3.0 Elements of SSEC Export Control Procedures

The following elements are intended to implement the SSEC Export Control Policy.

3.1 Defending our public domain exemption
We must have a clear idea of what is subject to export control and what is not in order to successfully comply with the regulations. Principal Investigators (PI) and Project Managers (PM) involved with projects in areas subject to control must therefore establish and maintain clear and complete records of the scope of what falls under “basic and applied research” and are encouraged to publish as much and as early as possible. In addition for formal publications, information placed in our library and publicly available is by definition in the public domain. “Public domain” is defined in section 120.11 of the ITAR. Project Managers and Principal Investigators are encouraged to document the development of projects and place copies of reports, technical descriptions, review materials, etc. in the library.

Public domain status cannot be claimed for anything subject to a non-disclosure agreement (NDA) nor anything obtained from outside sources (private company, government agency) not in the public domain. Research that is jointly pursued by the UW and government agencies or outside companies is public domain because it fits the ITAR public domain definition, unless we have we have incorporated information into our research activities which has been supplied by others under a non-disclosure agreement or identified as subject to the ITAR, or have agreed to accept restrictions on the publication of our research results.

The PI, PM, and the ISO Coordinator must collaborate to establish for each project a description of a) items and information subject to control (including all items subject to an NDA) and b) description of the areas of basic and applied research for which the research exemption applies.

Publication is encouraged. Frequent, contemporaneous informal reports can be used to document the public domain work and note the specific areas (without disclosing details) that are not in the public domain and thus are being protected.

### 3.2 Limit contact with items and information subject to export control

Obviously, the greater the contact with items and information subject to export control, the more difficult it becomes to make the case that our work is in the public domain. If an area of our research is determined to be subject to export controls, the effects could be severe and lasting. Consequences include: loss of the ability to publish or disclose results, not being able to participate in meetings open to non-US persons or organizations, and inability to work with non-US graduate students. These effects could effectively end active work in a given area. This has happened elsewhere.

It is important to reduce our contact with export sensitive information to the absolute minimum needed to carry on our work. Specific ways this might be done include:

- ask the government agency liaison (project manager, technical monitor) or a contact in a private company to research sensitive documents and provide the specific information needed rather than obtaining and searching the documents yourself.
- maintain the initiative when defining interfaces in sensitive areas to keep the information flow from “us to them” to the extent possible.

- minimize participation in meetings closed to non-US persons

- return unsolicited sensitive information to sender and notify the ECC so a record is made of the transaction for the file.

- Ideally, we would not allow any ITAR sensitive information in our work areas. This will require additional planning and effort but it will dramatically reduce our exposure to export control problems.

3.3 Handling items and information

3.3.1 Tangible (physical) items (e.g. hardware)

It would be difficult at best to properly control such items. If it became necessary to do so, we would have to draft a specific plan for the item in question.

3.3.2 Paper documents

Paper documents subject to ITAR control will be kept in the SSEC Library in a locked cabinet. They will be stamped with an ITAR identification so that material subject to ITAR control can be readily identified. A list of SSEC employees will be maintained who are “US persons” or who are exempt and thus eligible to use such documents. To the extent possible, only one copy will be maintained. If additional copies are absolutely necessary, they can be requested from the Library. The Library will maintain records of:
- the documents on file, when received, and from whom
- the number of copies made (a copy number will be marked on the doc)
- who checked out the document, when, and when returned.

Authorized individuals may check out documents but should return them promptly when their need has passed. Individuals should make every effort to minimize the number of documents in their possession and time they keep ITAR sensitive material.

The sources of paper documents are: documents from outside organizations which should be deposited in the library by the recipient as soon as received, paper copies of electronic documents (see 3.3.3 below), and possibly documents that we generate in the (rare) case that we must include protected information in a document.

3.3.3 Electronic Documents

Documents available on the web from sources that are protected for export reasons should be downloaded and printed by the SSEC Library and thereafter handled the same as paper documents.
Information on the web from protected sources that is not downloaded but only consulted should be done only by authorized individuals (US persons or exempt). All cases of use of these protected sources shall be reported to the SSEC ISO 9000 Coordinator (email is the preferred method) with the description of the reason and the information needed. The reason for maintaining a record of all such uses is to be able to defend the public domain research exemption by clearly showing what was consulted and why. The intent of the records would be to show a limited contact with sensitive information so as not to “contaminate” the public domain exemption.

3.3.4 Meetings involving ITAR sensitive material

Meetings here and at other facilities involving ITAR sensitive material require advance planning to maintain adequate elements of control.

3.3.4.1 Meetings held here

There must be reasonable minimum advance notice to all participants that ITAR sensitive information will be discussed to allow participants to plan whether or not to attend and if so, whom to send to the meeting.

The meeting participants must be advised at the beginning of the meeting and again just before any ITAR sensitive information is discussed that only authorized US persons and exempt persons are to participate.

A record of who attended the ITAR sensitive portions of the meeting shall be kept.

A record of what ITAR sensitive material was discussed shall be kept.

The meeting record shall be forwarded to the SSEC ISO 9000 Coordinator for filing.

3.3.4.2 Meetings held elsewhere

SSEC employees who attend meetings organized by others where matters subject to export control are expected to be discussed must meet with the ISO Coordinator before the meeting for a pre-meeting briefing which will include scheduling a post meeting debriefing. The pre-meeting briefing will include brief reminders of the important elements of our export control plan. The post meeting debriefing will review the documents received, any sensitive information discussed, and the information needed for the records.

If an SSEC employee finds that a meeting not expected to include information subject to export controls did in fact include export controlled information, a post meeting debriefing must be arranged as soon as possible. Please note the definition of what is included in ITAR is broad so being surprised by the content of a meeting should not occur often.
3.3.5 Standard of Care

The export control laws and regulations apply to individuals. That means the penalties apply to the individual, not the organization. Compliance is inherently the responsibility of the individual. SSEC employees are expected to know the law and regulations sufficiently to comply. Export sensitive information shall not be left out and visible when the employee is not in the immediate vicinity and in immediate control of the information. Employees shall not transmit export sensitive information orally, electronically, visually, or by any other means to persons not authorized to receive it, nor to persons who are not aware of the requirements of ITAR, and shall not transmit this information without identifying it as subject to export control. It is important to understand that, in contrast to the practice for classified information, export sensitive information is often not flagged because there is no requirement in the regulations to mark export sensitive material as such. Nevertheless, it is our duty under the laws and regulations, to recognize and protect the information.

3.3.6 Funding agencies, contractors, suppliers, project team organizations, and other outside organizations

Outside organizations should be advised as appropriate of our policy to minimize interaction with ITAR sensitive information in order to maintain our fundamental research public domain exemption. All SSEC projects shall seek to keep the information flow from SSEC to the outside organization to minimize the need for ITAR sensitive information as much as possible.

The primary method of informing outside organizations of our policy is to provide them with a copy of the policy itself, such as enclosing it in an application for research funding. Where outside organizations have not been supplied with this policy, or where specific concerns exist, they shall be advised that our export control procedures require advance notice of possible need to handle ITAR sensitive information. The purpose of this advance notice is to allow time to work out arrangements to minimize or eliminate our need to be exposed to such information. Outside organizations shall be advised that the University of Wisconsin is an open campus and that foreign nationals are normally present in our facilities. Therefore any export sensitive information should be clearly labeled as such and we should be advised before such information is transmitted so that we can give it appropriate protection. This export control document may be sent to outside organizations to communicate our control policies and procedures and may be used in response to AO requirements.

3.4 ISO Coordinator

The SSEC ISO Coordinator will be responsible for the implementation of this procedure with the support of all SSEC employees, will facilitate employee training and continuing awareness, will maintain the export control records described above, will monitor the implementation of this procedure, and will conduct internal audits and report the status of
our implementation to SSEC management. The ISO Coordinator will maintain appropriate contacts with others to keep our awareness of export control compliance current. The ISO Coordinator will schedule regular reviews with SSEC management and UW Madison Legal Services.

3.5 Training

All SSEC employees will be given the opportunity to attend briefings about the ITAR and our procedures for compliance. All new employees will be briefed upon beginning work at SSEC. Attendance at such briefings is a pre-requisite for access to export sensitive information.

All SSEC employees who do not meet the ITAR definition of “US Person” nor are eligible for the exemptions provided in ITAR shall also be briefed so they can assist to the extent possible in our compliance efforts and understand the requirements placed on those who are defined differently in ITAR. It must be emphasized that their help in our compliance efforts is necessary and appreciated as is their understanding of our need to comply with the law.

The Library has created a web page that contains all the information we have found about ITAR, the ITAR themselves, University of Wisconsin policies, and other related information. You can find it at: http://www.ssec.wisc.edu/library/itar.htm Everyone is encouraged to explore the information and ask questions. Questions may be directed to the SSEC ISO Coordinator. (erichards@ssec.wisc.edu)

Attachments:

A. The old rules (NSDD 189):

THE WHITE HOUSE
WASHINGTON
September 21, 1985

NATIONAL SECURITY DECISION DIRECTIVE 189

NATIONAL POLICY ON THE TRANSFER OF
SCIENTIFIC, TECHNICAL AND ENGINEERING INFORMATION

I. PURPOSE
This directive establishes national policy for controlling the flow of science, technology and engineering information produced in federally funded fundamental research at colleges, universities, and laboratories. Fundamental research is defined as follows:

“Fundamental research’ means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.”

II. BACKGROUND

The acquisition of advanced technology from the United States by the Eastern Bloc nations for the purpose of enhancing their military capabilities poses a significant threat to our national security. Intelligence studies indicate a small but significant target of the Eastern Bloc intelligence gathering effort is science and engineering research performed at universities and federal laboratories. At the same time, our leadership position in science and technology is an essential element in our economic and physical security. The strength of American science requires a research environment conducive to creativity, an environment in which the free exchange of ideas is a vital component.

In 1982, the Department of Defense and National Science Foundation sponsored a National Academy of Sciences study of the need for controls on scientific information. This study was chaired by Dr. Dale Corson, President Emeritus of Cornell University. It concluded that, while there has been a significant transfer of U.S. technology to the Soviet Union, the transfer has occurred through many routes with universities and open scientific communication of fundamental research being a minor contributor. Yet as the emerging government-university-industry partnership in research activities continues to grow, a more significant problem may well develop.

III. POLICY

It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts or cooperative agreements for
potential classification. No restriction may be placed upon the conduct or reporting of federally funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.

B. The new rules: the portion of the act that changed the NSDD 189 rules and most affected our activities:

PL 105-261, Div.A, Title XV
"Strom Thurmond Act of 1999" [excerpted]
Subtitle B--Satellite Export Controls

SEC. 1511. SENSE OF CONGRESS.

It is the sense of Congress that--

(1) United States business interests must not be placed above United States national security interests;

(2) United States foreign policy and the policies of the United States regarding commercial relations with other countries should affirm the importance of observing and adhering to the Missile Technology Control Regime (MTCR);

(3) the United States should encourage universal observance of the Guidelines to the Missile Technology Control Regime;

(4) the exportation or transfer of advanced communication satellites and related technologies from United States sources to foreign recipients should not increase the risks to the national security of the United States;

(5) due to the military sensitivity of the technologies involved, it is in the national security interests of the United States that United States satellites and related items be subject to the same export controls that apply under United States law and practices to munitions;

(6) the United States should not issue any blanket waiver of the suspensions contained in section 902 of the Foreign Relations Authorization Act, Fiscal Years 1990 and 1991 (Public Law 101-246), regarding the export of satellites of United States origin intended for launch from a launch vehicle owned by the People's Republic of China;

(7) the United States should pursue policies that protect and enhance the United States space launch industry; and

(8) the United States should not export to the People's Republic of China missile equipment or technology that would improve the missile or space launch capabilities of the People's Republic of China.

SEC. 1512. CERTIFICATION OF EXPORTS OF MISSILE EQUIPMENT OR TECHNOLOGY TO CHINA.

The President shall certify to the Congress at least 15 days in advance of any export to the People's Republic of China of missile equipment or technology (as defined in section 74 of the Arms Export Control Act (22 U.S.C. 2797c)) that--
(1) such export is not detrimental to the United States space launch industry; and
(2) the missile equipment or technology, including any indirect technical benefit that
could be derived from such export, will not measurably improve the missile or space
launch capabilities of the People's Republic of China.

SEC. 1513. SATELLITE CONTROLS UNDER THE UNITED STATES MUNITIONS
LIST.

(a) CONTROL OF SATELLITES ON THE UNITED STATES MUNITIONS LIST-
Notwithstanding any other provision of law, all satellites and related items that are on the
Commerce Control List of dual-use items in the Export Administration Regulations (15
CFR part 730 et seq.) on the date of the enactment of this Act shall be transferred to the
United States Munitions List and controlled under section 38 of the Arms Export Control
Act (22 U.S.C. 2778).