EXPORT CONTROL GUIDANCE:
STONY BROOK UNIVERSITY CREATED SOFTWARE AND ENCRYPTION

Introduction

This guidance addresses export control compliance pertaining to the publication and commercialization of software including, but not limited to, any research or scientific-purposed software or cryptographic software created by faculty, staff and students working at SBU. It also addresses technology and technical data associated with the development of this software ("software products"). Anyone who has already created software products or plans to create software products - - and in either case plans to publish or commercialize these types of products - - should adhere to this guidance. Even in the absence of the guidance contained herein, it is the responsibility of the individuals involved in these activities to be aware of the relevant export compliance regulations.

Point of Contact for Further Assistance

The Export Control Compliance Team is the point of contact for assistance with export control regulations and compliance.

- Contact the Export Control Compliance Team
- Export Control Compliance Website

How are Export Controls Applicable for Software?

Software (source and executable code) and cryptographic products have rules to govern these types of export activities, as well as what constitutes "publication" and "public domain" to either remove these items from the scope of U.S. export controls or render them subject to these controls.

- Even though SBU primarily conducts fundamental research (without sponsor or self-imposed publication or citizenship restrictions), the following rules apply.

Helpful Links:

- Stony Brook University Export Compliance Policy
- Department of State, International Traffic in Arms Regulations
- Department of Commerce, Export Administration Regulations

Why is Compliance Relating to Software so Critical?

Federal regulations relating to software exports are complicated. If a software author does not fully understand software publication and dissemination requirements or compliance responsibilities associated with the commercialization process, it can put the software's author and SBU at risk of incurring federal civil and criminal sanctions. These sanctions include substantial monetary penalties, federal debarment, and revocation of export privileges, and, where intentional circumvention of the exports laws is found, criminal prosecution. Higher educational institutions are a prominent focus of export enforcement. Your compliance with this guidance is critical to avoid these consequences.

So, What Exactly Do I Need to Know?

You should review the following four scenarios when sharing any software:

- Your software product (and the technology that developed it) is specially designed or modified for a military or defense end use such that it falls under the State Department's International Traffic in Arms Regulations (ITAR).
- You are (a) planning to make your software product publicly available by "publishing" i.e., placing it in the public domain1, or (b) commercializing the product through an invention disclosure and eventually licensing it; In the case of certain encryption software2 (software which contains cryptographic functionality), you plan to make the underlying source code publicly available (if so, then from a regulatory perspective, the executable code is considered publicly available).
- You plan to transfer/share the software product or underlying technology internationally at any point prior to publication, for example, as part of a software development collaboration with a non-U.S. institution or person.

The implications of these scenarios are discussed below.

ITAR Software

Under the ITAR software is broadly defined as any code, logic flow, algorithm, application program, or operating system, that is specially designed or capable of supporting the design, implementation, test, operation, diagnosis, or repair of a defense article. Broadly defined, a defense article is one that is specially designed or modified for defense purposes and satisfies the definition of articles that fall under the ITAR's U.S. Munitions List (USML) and related chapters.

Software that was not originally created for defense purposes can become ITAR-controlled if the original software is modified to accomplish a defense objective. In one potential example, if you have received source code through an NDA from a company or government agency that is considered a necessary background tool for your fundamental research project, and that code is actually used or incorporated into the development or compilation of resulting source code or executable code, the resulting code may be ITAR controlled.

Even if created as the result of fundamental research (without publication or citizenship restriction), software that is subject to ITAR jurisdiction cannot be automatically published or placed into the public domain. Software directly related to defense articles is considered a form of controlled technical data. There is a formal State Department process through which it is possible to seek a determination from State that the software does not rise to the level of a defense article and therefore is not subject to ITAR.

- While it is most unlikely that you would develop software subject to the ITAR (in part because SBU does not routinely accept publication/citizenship-restricted awards under Department of

[1]We note that there is often a conflated understanding of "public domain" and "open source" software, as these two terms are not interchangeable for EAR definitional purposes. Some open-source software meets the EAR definition of "published," while other open source software does not. It is important to vet all software, even "open source" software, against the EAR definition of "published" in order to determine the applicable controls.

[2] Certain types of less-sensitive cryptographic function are eligible for self-classification and export without encryption registration, while certain thresholds of cryptographic functionality (e.g., "strong" cryptography) trigger additional control requirements, as discussed in greater detail below.

Defense 6.3 or analogous funding), if you believe that you have created or are planning to create such software, contact the Export Control Compliance Team for further guidance.

- Technology (the result of fundamental research) leading to the development of ITAR-governed software may be published under certain circumstances; again, contact the Export Control Compliance Team prior to publication of such items for further guidance.

Assuming your software does not fall under ITAR, proceed to the next determination of whether you intend to publish the software and place it in the public domain, or commercialize it through the Intellectual Property Partners office (IPP).

"Published" Software (Non-encryption) versus "commercialized" software

Export Administration Regulations (EAR) Definition of Software

Under the EAR, software is defined as "a collection of one or more 'programs' or 'microprograms' fixed in any tangible medium of expression." Likewise, a program is defined as "a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer," and a microprogram is defined as "a sequence of elementary instructions, maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction into an instruction register." These items are listed on the Commodity Control List (CCL).

Note: The EAR controls items that are "dual use", items that, while not specially designed for defense purposes, have a level of inherent defense capability and are therefore considered export sensitive.

Published Software (Non-encryption)

Under the EAR, software (whether source or executable code) is considered published when it is available for general distribution either for free or at a price that does not exceed the cost of reproduction and distribution. (Reproduction and distribution costs may include variable and fixed allocations of overhead and normal profit for reproduction and distribution functions, but may not include recovery for development, design or acquisition of the software.)

Releasing the software as downloadable to the public at large without any cost recovery whatsoever removes the product from the scope of EAR and the end user restrictions. Under this arrangement, sometimes referred to as the "community model," the software is made available through a university- hosted web portal or alternative distribution site without visibility as to who is downloading the software, the country where the product is being used, or the ultimate end use.

When SBU recovers reproduction or distribution costs, SBU presumptively will have information as to who a potential end-user is (entity or individual), and, in the case of international requests, the country from which the download request is being made and processed. In this scenario, while the software still meets the criteria of being published and publicly available, SBU's knowledge of who is downloading the software and potentially where such end users are located triggers a significant export control compliance screening requirement.

This requirement makes it necessary for SBU to screen the user requesting the download to determine whether the user is identified on a U.S. Government watch list for end user restrictions

as well as to determine whether the user is located in a restricted, trade-embargoed country (currently, Iran, Cuba, Syria and Sudan). In either case (restricted end user or trade-embargoed country), a specific license from the U.S. Department of Commerce or the Treasury Department's Office of Foreign Assets Controls (OFAC) may be required before the download and cost recovery can occur, even if the software is controlled at the lowest level, known as EAR99.

Hence, if considering the option to release the product through a community model without any cost recovery versus seeking cost recovery and needing to screen potential end users, the former alternative is far preferable from an export risk and compliance burden perspective.

- SBU's IT support in concert with the Export Compliance Director will assist you in establishing a web-based dissemination portal.
- Any PI who wishes to recover costs for the reproduction/dissemination process should first seek further guidance from the Export Compliance Director who will facilitate the process and control procedure.

Note: even registering specific users through any sort of "Yes/No" selectivity filter without a monetary fee associated with such registration (e.g. requiring the registrant to agree to certain version control and/or dissemination restrictions) triggers the foregoing export control screening obligations. In this scenario, as with cost recovery, SBU gains knowledge of who the registrant is and potentially where located. Because of the advance screening requirement and extra compliance risk, PIs are strongly discouraged from pursuing this model.

- If you still believe that it is necessary to register your end user for reasons such as version control or attribution (even without cost recovery), please contact the Export Compliance Director prior to proceeding with such registration model.

In either case (whether freely downloadable distribution or cost recovery), there are two key caveats:

- In the event that, post publication, you are contacted by an individual or organization based in one of the OFAC trade-embargoed countries to provide advice or technical support on the software (such information not having been already posted on the web page or released with the product), this may constitute a controlled "service" which requires a specific license from the Treasury Department. In some cases, the nationality of the requestor or location of his/her affiliated entity may not be immediately apparent. In these cases, and prior to further engagement, contact the Export Compliance Director for assistance. If a license is necessary, the Export Compliance Director can assist in determining whether obtaining such a license would be viable.
- In the event that, post publication, you are contacted by an individual or organization seeking advice on how to apply the software for defense purposes, or the person identifies him/herself as a representative or affiliate of a non-U.S. defense organization (or if there is any indication that such query could lead to a non-civil end use of the software), contact the Export Compliance Director first prior to further engagement. Such activity could constitute a "defense service" which requires a license from the State Department.

With respect to the initial transfer of information from an industry sponsor to university researchers, that data is subject to the EAR where the parties have agreed that the sponsor may withhold from publication some or all of the information so provided.

Finally, please note that technology or data being used to develop a dual use or non-controlled software product ("development technology") can be published in scientific or industry journals, analogous to any other results of fundamental research.

- If necessary to transfer such development technology internationally prior to publication, please contact the Export Compliance Director prior to such transfer to ensure that no further compliance requirements are applicable.

"Commercialized" software

For any software that will be utilized with external partners, you are required to file an Invention Disclosure with Intellectual Property Partners (IPP) office.. Assuming IPP determines the product to be commercially viable for licensing purposes (which may include copyright registration and/or patent protection), the Export Control Compliance Team, in coordination with IPP , will classify the software for export control purposes.

If the software is dual-use controlled for certain countries, an export license will be needed to transfer the software to these countries. If the item is ITAR controlled, an export license will likewise be needed; such licenses are presumptively denied for particular countries for which ITAR items are strictly prohibited. In either case, OVPR would screen potential licensees against the U.S. Government Watch Lists to identify restricted end users for whom a commercial license may not be possible. Therefore, it is critical that you do not preliminarily transfer the software internationally for any reason (including technical review by an international party), as it may be subject to export control and require export authorization.

In the event that IPP returns the software product to you due to lack of commercial viability from SBU's institutional perspective, please note that any independent commercialization efforts you make would be outside the scope of your employment at SBU; you will be responsible for determining the export control implications of your product, including any export authorization requirements.

Publishing Encryption Software

Most publicly available software is not subject to the EAR. Certain publicly available encryption software, however, remains subject to the EAR. That is to say, publication of certain encryption software (software that contains or supports encryption functionality) is governed differently than publication of other software.

Under the EAR, there are varying degrees of control over EAR-controlled items which contain cryptography or are designed to use cryptography, and authorization requirements track to these degrees of sensitivity. For example, publicly available encryption software in object code with a symmetric key length of greater than 64-bits that meets the definition of "mass market" software

would carry a relatively lower level of control under the EAR. In contrast, software employing digital techniques performing any cryptographic function (other than authentication, digital signature, or execution of copy- protected software) with a symmetric algorithm employing a key length in excess of 56-bits, would carry a relatively higher level of control.

Some items are not treated as "encryption items" under the EAR and thus may not need to be evaluated for publishing in order to disseminate more freely under most circumstances. Such items would include those specifically designed for medical end use as well as certain select other items described in Note 4 to Category 5, Part 2—such as those with a primary function of information security, or those with functionality limited to IP or copyright protection.

Some encryption items are eligible for export to eligible end users and destinations under Encryption commodities, software and technology (License Exception ENC). Refer to Part 740.17 for a complete discussion of eligible items. Within License Exception ENC, some items which are less sensitive may be exported without required classification requests, reporting, or registration while other items require classification requests (or self-classification) and registration with the Department of Commerce/Bureau of Industry Security (BIS).

Further, some encryption software is authorized for export under Technology and Software Unrestricted (License Exception TSU). Refer to Part 740.13 for complete details. This Exception includes most mass-market software to most destinations, as well as encryption software items (both source and object code) that are considered publicly available.

In order to utilize License Exception TSU for publicly available encryption software that is subject to the EAR, it is necessary to first notify BIS at crypt@bis.doc.gov and the ENC Encryption Request Coordinator at NSA (National Security Agency) at enc@nsa.gov through email correspondence of the internet location (e.g. URL or internet location) of the publicly available encryption source code or by providing a copy of the software to them. Version updates or code modification also require updating these agencies through the same process. Where the source code is posted on the internet, you also must notify the BIS and the ENC Encryption Request Coordinator each time the internet location is changed.

- Given this special procedure for encryption software, please contact the Export Compliance Director in advance of the notification procedure: she will help guide you through the necessary steps. It is critical to follow this procedure, even if you believe that a similar cryptographic functionality already exists in the public domain.

Mass market encryption software that is classified under ECCN 5D992 requires the submission to BIS of a one-time encryption registration (in advance of publication) as well as an annual self-classification report. Once the software is properly self-classified as "mass market" and initial registration has been submitted to BIS, the subsequent publication of the software will render it outside the scope of the EAR and any watch list screening and end user restriction requirements. However, the same restrictions to providing "service" on the software, under OFAC (sanctioned countries), ITAR, and the EAR (i.e. defense service restrictions) apply to encryption software in the public domain as with non-encryption software discussed above.

International Transfer of Unpublished Software

Regardless of whether or not the software contains cryptographic functionality, you should be aware that any product that has not yet been placed into the public domain through one of the foregoing methods remains potentially subject to the EAR or ITAR licensing regulations.

It is a serious export control violation to transfer a software product (by any medium) to a destination that requires an export license prior to receiving that authorization. For example, in the instance that you are co-developing a software product internationally, even transferring the U.S.-origin portion of the source or object code to the collaborator could, depending on the nature and end use of the software, trigger an export authorization requirement.

- Hence, if you believe that it will be necessary to transfer your software product (or portions of the code) to an international collaborator, first contact the Export Compliance Director who will identify any applicable control requirements. This is true even if you believe that there is already commercial likeness or availability to the type of software product you are working on within or outside the United States.
- When traveling with an unpublished software product that resides on your laptop hard drive or other hand-held device: the laptop or device then assumes the level of export control that the software product is subject to and may require prior authorization or a specific exemption for international travel purposes. Contact the Export Compliance Director in advance of international travel plans if this scenario is applicable.

Conclusion

Complying with this Export Control Guidance on Software and Encryption will minimize your export risk greatly. In some cases, determinations under this guidance may be complex; therefore, it is critically important to contact the Export Control Compliance Team with any questions concerning the disposition of your software product. Please share or refer to this guidance with those in your department who are likewise involved in the software development process.

###