III. LICENSE EXCEPTIONS FOR UNIVERSITY RESEARCH

Much of the research and education activities taking place at Mines are excluded from export controls because universities often may assert a Fundamental Research Exception. The exceptions, however, must meet the legal definitions and analysis. Note: **The FRE is not an automatic exception or exclusion; working at a University or on a University project does not magically mean ITAR or EAR does not apply.** Thus please consult with ORA and/or Office of Compliance.

A. Fundamental Research Exception (FRE)

The *Fundamental Research Exception* (FRE) in both EAR and ITAR pertains to research (basic or applied) in science, engineering, and mathematics performed or conducted at an accredited institution of higher learning ("University") in the U.S., where the results will be published and shared broadly in the scientific community (and under the EAR where the resulting information has been or is about to be published). The provisions for the FRE are somewhat different when comparing EAR (covering Dual Use goods and technology, predominately for commercial use, but possibly with military use) and ITAR (covering Defense Articles, Services and technology--design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of item). Thus, attention to definitions and activities must be considered when examining whether a FRE exists and under what applicable statute it is analyzed. The BIS commentary tells us that university-based research may be presumed to be fundamental research, however, it is a rebuttable presumption (i.e., where the research is not within the scope of technology and software that arises during, or resulst from fundamental research. See 15 CFR § 734.8.

Some things are the same under the FRE analyses under EAR and ITAR, including:

1. **FRE is not restricted**. Fundamental Research is distinguished from research that results in information restricted for proprietary reasons or national security reasons or pursuant to specific U.S. government access and dissemination controls.

2. **FRE freely publishes**. If the subject of review involves a contract/agreement with publication restrictions of any type (including pre-publication approvals), for other than the sponsor's review of its proprietary information on a temporary, short-term basis (e.g., patent filing window), then fundamental research exception to export controls or licensing may not be relied upon.

Thus, ORA works to maintain this important Fundamental Research Exceptions on behalf of the entire University, as well as the individual PI, in the contractual terms and conditions.

B. Other Exclusions

1. **Public Domain**. *Public Domain* is the term used for information that is *published and generally accessible or available* to the public through a variety of means. Both the EAR and ITAR provide that no license is needed to disclose technical information to foreign nationals inside the United States in classes or laboratories, at conferences, or in publications, *if the information is in the public domain*. In fact, just because an item or activity is subject to the EAR does not mean that a license or other requirement automatically applies. A license or other requirement applies only in those cases where other parts of the EAR impose a licensing or other requirement on such items or activities." *Emphasis added*. See 15 CFR §734.2(a)(3).

a. Public Domain is defined differently under EAR & ITAR.
To be in the Public Domain, the following applies:

- EAR requires that the information has been, is about to be, or is ordinarily published. (EAR, 15 CFR 732.2, 734.7);
- ITAR requires that the information *has been* published (ITAR, 22 CFR 120.11(8)).

b. "Publicly Available" software not necessarily an Exclusion.
Under EAR, publicly available has different meanings for software; encryption technology may be publicly available, and yet the technology may not be in the public domain. Mass Market software that might otherwise be exported under License Exception ***TSU*** (technology and software) is not eligible for treatment as an exception, if the software includes encryption capability as described in certain ECCNs. Encryption software is eligible for a "tools of the trade" License Exception for temporary exports (***TMP*** ***or BAG***), e.g., taking it along on a business trip in a notebook computer, as long as the required conditions for that License Exception are met. BIS has an excellent Encryption FAQ resource page on the web.

Please consult ORA or Office of Compliance for more information.

3. **Limitations of FRE/Public Domain**
The fundamental research and public domain exclusions apply only to information or technical data. The exclusions do not apply to articles, things (e.g., physical items including specified scientific equipment, etc.) or services (e.g., training foreign nationals inside or outside the United States). Other exemptions may apply to exports of equipment and services, even if the fundamental or public domain exemptions do not. For example, use of public domain information might be considered a defense service and thus require a license from a government agency, if the information is part of a covered activity (e.g., teaching foreign military about the public domain information relating to a defense article, see 22 CFR 120.9(a), Defense Service definition).

Public domain information is excluded from control as ITAR technical data. Open source information or code though available to the public is not "public domain" just because an owner provides the software or technology publicly and generally accessible. The software or code available as "open source" is only provided under a grant of rights (license). Thus, it cannot be "public domain".

4. **Public Information Exclusion.** Public Information Exclusion refers to information that *is already published* or *is out in the public domain* is considered public information and, as provided for under the EARs is **NOT** subject to export controls. Examples of information in the public domain include, but is not limited to:

- Books, newspapers, pamphlets;
- Readily available materials at libraries open to the public or at university libraries;
- Publically available technology and software;
- Information presented at open conferences, meetings, and seminars open to the public;
- Information included in published patents; and
- Websites freely accessible by the public. See 15 CFR§734.7 and §734.10.

5. **Loss of FRE**
If a researcher or employee agrees to a "side-deal" (for example, not to publish even though the Mines agreement with a sponsor identified that Mines is freely available to publish), then the FRE would be lost

and the research may be subject to export controls.

C. Educational Information Exclusion

The Educational Information Exclusion refers to information that is normally taught or released by the university as part of the normal instruction in a catalog course or in an associated teaching laboratory. This information may be considered Educational Information and the federal regulations may **NOT** cover this information under export controls. See 15 CFR §734.9. Note: The regularly taught in a college level course may require review with ORA or Compliance as not all areas are assumed to be covered as "Educational Information." For example, continuing education courses are not necessarily the same as undergraduate courses for enrolled students.

D. Encryption under EAR.

Encryption or encryption functionality comes packaged in almost all devices today that have a computing functionality or structure. Similar to other products or items, though, some software encryption export controls are "within scope" (requiring a classification and license) and some products/items are not within scope under the EAR.[3] Items or products that have encryption (or the ability to encrypt data) include things that have an operating system, such as, but not limited to, cell phones, routers, network infrastructure, Point of Sale/credit card devices, wireless keyboards, laptops, tablets, etc. (AEUCO 2016 conference).

1. **Review Encryption for License**.

Generally, we review encryption for EAR license/regulatory coverage, such as:

a What's within Scope?
b. Is it excluded from the regulations? Specific exclusion such as medical devices or under fundamental research exception?
c. Are we dealing with Published Information? (E.g., in a University library?)
d. Is the Educational Information Exclusion available (i.e., does not apply to ECCN 5D002 software, except when published/publicly available object code)?
e. Does this impact research or funding source? (Exclusions do not cover some types of encryption)
f. Will the code be published eventually?
g. Will the encryption be hand-carried out of country? Certain encryption software remains subject to EAR even if published.

2. Other Options to Encryption Licenses.

Some options to being under the EAR requirements due to encryption, e.g., or "de-controls", may apply to exclude encryption; however, these options require analysis and documentation. Recall, the ability to encrypt data is not the only thing that brings Encryption within scope of the EAR. Thus, we need to identify if the "de-controls" attach to the item or product containing encryption, so the encryption functionality may be considered out of scope. This may include an analysis as follows:

a. Is the item/product ***medical end-use***? (mostly exempted from EAR coverage);

[3] Note: Encryption used to be covered under ITAR, however, it is under the EAR, which does not exclude it from review for scope and license.

b. What is the "***Primary Function***" of your product? (depending on the primary function, the product may escape EAR coverage). The function is not primary, if the main function of the encryption is not for one of the following four (4) activities:

1). Information security;
2). Computing;
3). Communicating; or
4). Networking.

c. When the encryption is not primarily one of the 4 items above and thus under EAR, determine if the software or technology is covered by ***EAR99***?

d. Does the "***Dormant Encryption***" exception apply? (e.g., product has an encryption chip in it, however, the functionality/code does not use this functionality, so product becomes EAR classification, ECCN 5D992, such as virus protection software that has encryption software)

e. Does the "***Mass Market***" exemption apply? (e.g., items that are sold from stock, online selling points, etc., and product available to general public and using standard encryption), so many apps, cell phones, tablets, most likely a 5D992 Mass Market exemption. Applications, aka "App" being developed for mass market that have encryption functionality require review by BIS in limited circumstances and when they provide encryption functionality in another item (e.g., chip). Mass market app using non-standard or proprietary encryption functionality (must review what meets "non-standard crypto") would require BIS review.

f. End-user, end-use or country of transfer? The end-user and ultimate location of the end-use is part of the inquiry as well.

3. **Controlled Items that need License May Sometimes Use Exceptions.**

License exceptions and consideration are somewhat different under Encryption and we do not necessarily start with FRE review. These include the following 4 exceptions for review in Encryption/Cryptography:

1). ENC— encryption;
2). TMP—temporary exception (professional use laptops);
3). BAG—baggage exception (personal use laptops); or
4). TSU: occasionally used for specific open source published software. See Ear §740.

To use the ENC Exception, BIS has a submission process for an entity to submit an encryption registration under Mass Market Exemption, and the applicant can receive approval from BIS to self-classify the product. This must be done at least once, when originally applied for and then an annual report sent to BIS of all the products we self-classify in that calendar year follows.

4. **Common topics affecting Faculty:**

a.***Traveling abroad with Laptop?:***

What questions do I need to ask when I want to travel abroad with a laptop?

1). Where am I traveling? (certain countries have restrictions, sanctions or embargoes, E.g., need license on mass-market encryption; if going to N. Korea, Iran, Sudan, Syria, and Cuba* may not be able to take it there because of embargo/sanction)

2) What is the type/inventory of software on the laptop and what does it do?

a) *Inquire about USML/ECCN number*. Did the manufacturer put classification of the laptop or operating systems on their website? (E.g., Microsoft Windows 10 is 5D992 and "Mass Market" exception. Apple is similar at their website; Redhat, using Linux 5D992 ENC unrestricted and they list number of commodity classifications/C-Cats.)

b). *Trust but Verify*, is the Manufacturer correct on the assigned ECCN (by checking with ORA and using the software to review the item/product)?

c) *Take Paperwork with you*. If a license can be completed, fill out the paperwork and travel with the documentation (either from BIS or the self-classification of an exception).

3) Consider the Usage/Access to Data. The laptop may be approved to go with faculty under an exception, however, the Data coming across the laptop while abroad may not be approved under the license exception. ***Ask the question*** of what data you can receive/access via email or home file directory access while abroad?

b. Traveling abroad with Smartphone *(iPhone, Android phone, Etc.)* do I need a license for the encryption in the phone?

1) Where are you traveling? Restricted or embargoed location?
2) Does a license exception *such as Mass Market apply to the software/item?
Often the Mass Market exception applies for smartphone, however ECCN 5D002 classification of software "unrestricted" may be on the website.

Note: If the company/manufacturer website uses incorrect language (e.g., "5D002 restricted") there is necessity to review more thoroughly with ORA or Compliance.

c. ***Exports to the "Cloud".***

Under the BIS Final Rule to harmonize and reform Export Controls (effective September 1, 2016), the agency provides a Safe Harbor for entities regarding certain electronic data subject to the EAR not being considered an "Export," if stored in the cloud outside the U.S. In order to qualify for the Safe Harbor, (and excluding ITAR technical data/information, etc.), the transmitting or storing electronic data that meet certain security standards would not constitute an Export of that data, provided that the technology or software is:

1) Unclassified;
2) Secured using "end-to-end encryption";
3) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or other equally or more effective cryptographic means; and
4) Not intentionally stored in a military-embargoed country or in the Russian Federation.

d. ***Decryption.***

BIS includes a definition for "access information," which is information (like decryption keys, network access codes and passwords) that would allow access to encrypted technology and software in unencrypted form. Such access information is subject to the same level of Export Controls as the data being accessed if the data were unencrypted. Note:

e. ***Data Breach/Loss.*** Any member of the Mines' community is required to report the loss, breach, or unintended access to technical data or private data. Please consult the Office of Compliance for further direction on how to address a loss of Mines' data. Generally, a data breach is not an export control issue for the victim; however, the steps for Safe Harbor should be applied to all private or export controlled data to avoid an accidental Export.

[End of Section]