Export Control Guidance for Remote Work

Due to the OVPR's recent recommendations that research activities be conducted remotely, the Export Compliance Group is mindful of changing circumstances as they relate to safeguarding export-controlled technology. See the guidance below regarding remote access and work involving export-controlled technology depending on if you are conducting research domestically or outside of the US. Please note that this guidance is responsive to the current COVID-19 emergency situation necessitating remote working arrangements, and is subject to change in light of changing laws, regulations and university policies. Upon return to normal working conditions, please resume usual procedures for safeguarding export-controlled data.

Due to CMU's open campus environment, any projects generating or using export-controlled information would generally have been coordinated by or with the involvement of the Export Compliance Group. However, if you were unexpectedly given access to information or materials you believe to be export-controlled, or if you believe you are generating export-controlled information on a project that is not otherwise being managed in coordination with our office (through a Technology Control Plan or otherwise), please appropriately safeguard the information in accordance with this guidance and contact our office for assistance.

IMPORTANT NOTE*: This is general guidance regarding safeguarding unclassified export-controlled information and may not be applicable to every situation. If this guidance conflicts with an applicable Technology Control Plan, export control attestation, sponsored research agreement, or other type of agreement or policy that contains more restrictive requirements, you must follow the more restrictive terms of the applicable agreement or policy (including but not limited to any applicable policies, procedures, requirements of Carnegie Mellon's Software Engineering Institute, which would supersede this guidance). If your Technology Control Plan is less restrictive or you have specific questions, please contact the Export Compliance Group (ECG)ECG (export-compliance@andrew.cmu.edu).*

Inside US

Remote access and work: We recommend that all research generating or involving access to export-controlled information be conducted over a CMU-sponsored VPN. i.e. using CMU's General Campus VPN (https://www.cmu.edu/computing/services/endpoint/network-access/vpn/index.html) to access the CMU machines or servers you typically use for your work, or using a VPN that CMU has arranged to enable your access to export-controlled information through a third party's site or servers.

As a reminder, if new data is generated from the use of export-controlled data, this new data may also be export controlled. The originators of such export-controlled data should be marking this information as "export controlled" and should be treating it the same way as the original export-controlled data used in the work.

Export-controlled information accessed or generated should not be saved to a computer's hard drive or a cloud server that was not already approved in a relevant agreement or otherwise by CMU's Information Security Office and Export Compliance Group for use with export-controlled information.

Digitizing hard copies of export-controlled information: Do not scan or digitize hard copies of export-controlled materials on unauthorized scanners. Please contact our office if you are unsure which

scanners may be used. Once the controlled hard copies are converted into digital materials, they should be treated with the same level of restricted access as the underlying hard copies.

Digital sharing: The best way to access or share export-controlled data (drawings, test data, 3D drawings etc.) is to upload it to a secure, CMU file system or server and instruct the authorized recipient to access it through VPN as described above. Using CMU's enterprise Box account (see https://login.cmu.edu/idp/profile/SAML2/POST/SSO?execution=e2s1) is another secure method of sharing export-controlled information, though please be mindful of who has access to the particular Box folder and the privileges being granted to them through Box. Access should only be granted to authorized individuals with a need to know (e.g. relevant individuals named in a relevant Technology Control Plan, or individuals our office has otherwise confirmed are permitted to access the information under the relevant export control laws and regulations) and with the most limited privileges needed for their contemplated access and use. We do not recommend using email as a method to send export-controlled attachments. Also, as mentioned below, we do not recommend using Zoom's file sharing feature. Please work with the Export Compliance Group if your methods for data access or sharing cannot conform to these recommendations.

Teleconferencing: When sharing export-controlled information, we recommend using an audio-only method. Due to Zoom's encryption limitations, screen sharing and video conferencing are not supported as a recommended methods of sharing export-controlled information. Individuals sharing export-controlled data over the phone should be mindful of participants on the call (e.g. ensuring they are only the relevant individuals named in a relevant Technology Control Plan or individuals who our office has otherwise confirmed can appropriately access the information). Please observe the digital sharing guidance provided above to share files.

Recommendations for all cases:

- Be aware of your surroundings (i.e., access information and conduct calls in settings where you can ensure that unauthorized persons or active digital assistants are not privy to the details of the conversations and/or are able to view your screen);
- Avoid using shared computers, or if you must, have a separate login for yourself that does not have administrative privileges;
- NEVER save research files on your personal hard drive or personal cloud storage;
- Apply all patches available for your operating system and applications; and
- Make sure there is anti-malware software running (where possible).

Outside US

If you are conducting research outside of the US, or if you intend to make export-controlled information available to someone outside the U.S., please consult with Export (export-compliance@andrew.cmu.edu) and the Office of Sponsored Programs (OSP@andrew.cmu.edu).

The Export Compliance Group will continue to provide any updates and changes to export rules and regulations to the OVPR. Please contact the team at Export-Compliance@andrew.cmu.edu with any questions.