UMSL University of Missouri–St. Louis

Research Security and Export Controls INFORMATION SHEET

The University of Missouri System is committed to complying with export control and sanctions regulations and has adopted these principles into its Collected Rules and Regulations[1].

Research Security and Compliance (RSC) is responsible for reviewing all sponsored agreements funded by the Department of Defense (DOD), NASA, U.S. Intelligence Agencies, and the Department of Energy (DOE) because of the likelihood that these agreements will need to comply with export control regulations, such as the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR)[2].

This document contains guidance from RSC on steps that can be taken at the proposal stage to:

- Minimize the impact of export control restrictions on this type of federal work; and
- Build appropriate cost expectations into research budgets, and plan for the use of only U.S. Persons (U.S. Citizens, U.S. Permanent Resident, or those on certain special statuses like refugees and asylees) or licensed Foreign Persons (generally those in the U.S. on an approved visa and citizens of other countries located outside the U.S.) in the project.

Before submitting any federally funded research proposal in which the University will participate as either the prime contractor or a subcontractor, RSC recommends the solicitation be reviewed for references to:

- Export controls;
- Security requirements;
- Controlled Unclassified Information; and
- "Fundamental Research."

Unless Sponsored Programs has "scoped and negotiated" the project as "Fundamental Research" with the sponsor, clauses in DOD, NASA, and DOE awards may automatically restrict the publication of research results; limit the participation of Foreign Persons on the project team; and/or impose onerous information security requirements.

Fundamental Research as defined in the ITAR at 22 CFR § 120.34(8):

"Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept otherrestrictions on publication of scientific and technical information resulting from the project or activity; or

(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

The research must be conducted by an accredited institution of higher learning in the U.S."

References to "export controlled," "ITAR," "EAR," "Controlled Unclassified Information (CUI)," "Covered Defense Information (CDI)," "Controlled Technical Information (CTI)," "Cybersecurity Maturity Model Certification (CMMC)," "NIST 800-171," "DFARS 252.204-7012," or "Distribution Statements" **indicate there is a high likelihood that your research will not be Fundamental Research and will be considered Restricted Research**.

If funded, additional costs will need to be planned for in the project budget. All project personnel (including students) will need a secure space to conduct Restricted Research.

Please note: If your project working with exportcontrolled or other restricted information is funded, we will be working together to help ensure all your compliance needs are met. Your contacts:

Research Security and Compliance
Danielle.Hunter@umsl.edu

[1] *CRR 430.020 Export Control and Sanctions Compliance*

[2] *UM System Export Compliance Management Program*

Research Information Security Team
umresearchsecurityteam@umsystem.edu **It is important to note that if the University accepts restrictions on either publication or access by foreign persons, a project will not meet the definition of Fundamental Research and potentially becomes Restricted Research.**

Engaging in non-fundamental ("restricted") research potentially prevents members of the University's international community from participating in the project and would limit graduate students' theses or dissertations (impacting their ability to graduate), including U.S. Person graduate students.

In addition, accepting a Restricted Research project requires that administrative and technical compliance procedures be established to prevent the unauthorized disclosure of research results. These procedures include the implementation of a Technology Control Plan (TCP) and application of information security protocols, the costs of which will need to be borne by the sponsored project. These administrative and technical compliance procedures must be implemented before the execution of any award agreement.

Starting in 2024, the federal government will require external auditors to review institutions' cybersecurity related to conducting Restricted Research to ensure they are complying with the regulations listed above. If, after reading the guidance below you are unsure whether your research may be subject to these types of requirements, reach out to the Research Security and Compliance Team.

Fundamental Research

If a Principal Investigator believes their proposed research should meet the definition of Fundamental Research, **one of the following statements must be included in the cover sheet and/or proposal document** to notify sponsors early in the award process and to assist Sponsored Programs with award negotiations.

The University as a prime contractor:
"National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical, and Engineering Information" established national policy that, to the maximum extent possible, the products of fundamental research remain unrestricted. The University asserts that the research proposed in the scope of work should be considered Fundamental Research and anticipates there will be no restrictions on publication or the involvement of foreign researchers, or other requirements in the award that would limit disclosure of the research results."

The University as a subcontractor:
"National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical, and Engineering Information" established national policy that, to the maximum extent possible, the products of fundamental research remain unrestricted. The University is submitting this proposal and participating in this project based on the condition that the research can be conducted as fundamental research. The University requests that the offeror/prime contractor use its best efforts to negotiate provisions in the prime contract to accommodate this subcontract as fundamental research or obtain such written certification from the federal funding agency's Contracting Officer that allows the University to perform their effort as Fundamental Research, ensuring that any DOD restrictions on access or dissemination in the prime contract to not flow down to the University."

Restricted Research

If there is not a Fundamental Research assertion in the proposal and the solicitation includes any indications of the possibility of Restricted Research, plan on including additional costs in the budget.

In addition to the implementation of a Technology Control Plan (TCP), all systems that receive, process, and store project data will need to meet additional administrative and technical security requirements, and all project personnel working with export-controlled information will need a secure computing environment in which to conduct their work.

Secure computing environments receiving, processing, and storing restricted data will be subject to external compliance audit investigators starting in 2024. **Standard tools like Microsoft Office 365, Box, and OneDrive do not meet data security requirements** for conducting this type of work, nor do standard University-issued desktops and laptops.

To meet these audit requirements, the University of Missouri System provides Arculus, a hosted Microsoft Azure GCC High Environment[3], which provides a version of common productivity tools that meet these data security requirements, like Outlook, SharePoint, Microsoft Office, etc. Additionally, Arculus provides a virtual desktop so that all restricted data received, processed, and stored by the University can be handled in a secured environment. A standard license for Arculus with the virtual machine is an annual cost of $1,912.20/year. Included in this package: Virtual Machine (desktop in the cloud), 4 vCPU, 16 GB RAM, 128 GB SSD, 160 hours of monthly usage, and Secure Office 365 Suite.

[3] *Office 365 GCC High and DOD*

Additional cloud computing resources are available. The costs for additional services are variable based on usage. If the standard offering in GCC High will not meet your needs and your proposal is likely to be funded, please visit the Microsoft Azure Pricing Calculator or contact the Research Information Security Team to discuss your technology needs and obtain more information about the costs to include in your budget.