Stony Brook University

Research Security Program

You should read this message from the Research Security Program if you are:

- Faculty who have or plan to have international relationships/activities, especially with China, Russia, or Belarus
- Faculty who have or plan to have federally funded research
- Deans and chairs who have faculty involved or interested in these activities

About Stony Brook University (SBU) Research Security Program

The Research Security Program supports researchers in international engagement and global activities. The three main areas of importance are (1) **disclosure** - disclosure of external relationships in accordance with applicable federal sponsor guidance and SBU policy; (2) **protection** - protection of intellectual property, research data, and materials (cybersecurity, physical security, and review of international relationships and high risk activities), and (3) **export controls** -a broad body of federal regulations that regulate the transfer (in any manner) of controlled information and items.

Important Information on U.S. Government Actions that Pertain to Research Security

International Relationships/Activities Updates

- Know your Collaborator/Partner

Department of Defense Updates the1286 List

The Department of Defense has updated the1286 List. As a reminder, the 1286 List identifies those foreign institutions that have been confirmed as engaging in problematic activity as described in the National Defense Authorization Act (2022) and identifies foreign talent programs that have been confirmed as posing a threat to the U.S. as described in the referenced law. More information on Foreign Talent Programs

- The 1286 List is just one of several U.S. government lists of entities and persons who are restricted and/or denied certain transactions (Restricted Parties). Read more about Restricted Parties here.
- All foreign persons and entities must be screened for inclusion on any of these lists prior to engaging in activities. See how to conduct a restricted party screening using Descartes Visual Compliance software.

Important: International activities with any of persons or entities (including higher education institutions) listed on a Restricted Party List must be reviewed by the Research Security Program.

Increasing Controls and Restrictions with Russia and Belarus

On June 12, 2024, the U.S. Departments of Treasury, State, and Commerce imposed new restrictions targeting Russia. Export regulations regarding Russia are increasingly complex.

Important: Contact the Research Security Program before engaging in activities that require the transfer of non-public information or any items to Russia or Belarus.

U.S. Government Prohibitions on Certain Suppliers/Products

- Restricted Purchases

The U.S. Government Bans on Security Related Products

The U.S. government has issued bans on both foreign and U.S. subsidiary companies for sale and use (in federal awards) of security related products. These requirements may be applied broadly by federal agencies and are included in all federal contracts and subcontracts.

- Kapersky Lab, Inc., a U.S. subsidiary of a Russia-based anti-virus software and cybersecurity company, prohibited from directly or indirectly providing anti-virus software and cybersecurity products or services in the United States or to U.S. persons. The prohibition also applies to Kaspersky Lab, Inc.'s affiliates, subsidiaries and parent companies (together with Kaspersky Lab, Inc., "Kaspersky").
- ZTE Corporation, Zhejiang Dahua Technology, Co., Huawei Investment and Holding Co., Hangzhou Hikvision Digital Technology, Co., Hytera Communications Corporation for telecommunications and surveillance equipment. This includes all of their affiliates, subsidiaries wherever located.

Important: SBU prohibits products made by or sold by these companies. In addition, they are not allowed to be used on federal awards.

Federal Contracts and Subcontracts - ByteDance/TikTok Prohibition

-Social Media Applications - Personal and University Owned Devices

U.S. Government Bans ByteDance Applications

ByteDance - TikTok applications are banned from use on electronic devices that are used in any manner, including personal cell phones and laptops, on federal contracts and subcontracts that contain the restriction.

Important: If you have a federal contract or subcontract, review the Federal Acquisition Regulation clauses for compliance requirements. The Office of Sponsored Programs or the Research Security Program can assist with explaining requirements.

Office of Science and Technology Policy (OSTP) Releases Final Guidance on Research Security Programs

- What this means for SBU

Guidelines for Research Security Programs at Covered Institutions (Guidance)

On July 9, 2024, the Office of Science and Technology Policy (OSTP) released the final Guidance for Research Security Programs at Covered Institutions in accordance with National Security Presidential Memorandum 33 (NSPM-33).

SBU, as a Covered Institution, will be required to implement cybersecurity standards, foreign travel security, research security training, and export control training in compliance with U.S. federal regulations and sponsor policies. The Research Security Program will be coordinating compliance of new requirements with other key areas on campus. Further communications will follow.

Important: Watch for future communications from the Research Security Program containing information and resources about the program!

Research Security Training Now Available

- Currently Optional but Highly Recommended

Research Security Training Now Available

Make sure to read the important note below about how to take this training!

The U.S. National Science Foundation, in partnership with the National Institutes of Health, the Department of Energy and the Department of Defense, created research security training for the research community (NSF Training). This training provides recipients of federal research funding with information on risks and threats to the global research ecosystem — and the knowledge and tools necessary to protect against these risks. The training includes four interactive video modules.

Important: SBU has the NSF Research Security Training available in Collaborative Institutional Training Institute (CITI). Faculty and staff are strongly encouraged to complete the training in CITI* to create an institutional record of training completion as this training may become mandatory by federal sponsors.

*CITI is available to all SBU faculty, staff and students - Use the Log In Through My Organization option and use your NetID and password. Directions: Select "Add a Course", then "I want to complete the Research Security Course at this time", then "Research Security Training", select "Next". You will then have the option of viewing any or all four modules, completion of the modules will be recorded in CITI.

Questions about the content provided here or about research security, reply to this message, contact the Research Security Program, or visit the Research Security Program website.

Thank you,

Susan Gasparo
Director of Research Security
Office of the Vice-President for Research