Last updated: 12/01/2025

Research Security Overview

Purpose/Background

In alignment with the CHIPS and Science Act of 2022 (P.L. 117-167) and National Security Presidential Memorandum-33 (NSPM-33) which aim to safeguard US science and engineering research, and to comply with Federal funding requirements, Bates College has implemented several policies focused on ensuring Research Security. These policies and procedures identify requirements for training and disclosures for Bates faculty and staff to remain in compliance with Research Security requirements of federal funding agencies.

Overview

Research Security compliance at Bates includes the following policies and associated training requirements:

- Policy on Research Security and Disclosure of Other Support
- Training in the Responsible and Ethical Conduct of Research
- Policy on Malign Foreign Talent Recruitment Programs

In addition, the following policies are relevant to faculty who travel internationally on Bates business and are included here for reference.

- Financial Conflict of Interest Disclosure requirements
- Export Control
- Foreign Travel

Each of these policies meets a specific federal funding compliance requirement and serves a specific purpose, however there is overlap in their purposes and implementation processes and training requirements. Faculty and staff who wish to apply for external funding are advised to consult with the Office of Research and Sponsored Programs (ORSP) for guidance specific to the training and disclosure requirements for their proposed funding agency. See this TABLE for training and disclosure requirements and timing by funder.

Last updated: 12/01/2025

Policy on Research Security and Disclosure of "Other Support"

Effective Date: October 10, 2025

Purpose/Background

- This policy identifies requirements for training and disclosures by Bates faculty and staff who wish to apply for federal funding so that they and Bates remain in compliance with Research Security and Other Support Disclosure requirements of federal funding agencies.
- This policy complies with Federal funding requirements in alignment with NSF Important Notice No. 149, NIH Notices NOT-OD-25-133, and NOT-OD-21-073 and Department of Energy Financial Assistance Letters No. FAL 2022-04 and No. FAL 2025-02 and with the CHIPS and Science Act of 2022 (P.L. 117-167) and National Security Presidential Memorandum-33 (NSPM-33)

Research Security regulations aim to safeguard US science and engineering research from inappropriate influence and conflicts of interest. To maintain the integrity of, and public trust in, the research enterprise, funding agencies require that researchers

1. undertake training in identifying and preventing potential threats to their research and
2. disclose all resources made available to the researcher in support of and/or related to all of their research endeavors, regardless of whether or not they have monetary value and regardless of whether they are based at the institution the researcher identifies for their current grant.

This information is reviewed by funding agency staff to ensure the following:

- Sufficient levels of effort are committed to the project.
- There is no scientific, budgetary, or commitment overlap.
    - Scientific overlap occurs when (1) substantially the same research is proposed in more than one application or is submitted to two or more funding sources for review and funding consideration or (2) a specific research objective and the research design for accomplishing the objective are the same or closely related in two or more applications or awards, regardless of the funding source.
    - Budgetary overlap occurs when duplicate or equivalent budgetary items (e.g., equipment, salaries) are requested in an application but already are provided by another source.
    - Commitment overlap occurs when an individual's time commitment exceeds 100 percent, whether or not salary support is requested in the application.
- Only funds necessary for the approved project are included in the award.
- Any foreign resources that meet the definition of a foreign component have received appropriate prior approval.

These trainings and disclosures help ensure transparency and the integrity of the US science and engineering research enterprise.

Last updated: 12/01/2025

Policy Statement

Part I: Training

Principal Investigators (PIs), co-Principal Investigators (co-PIs), and any individual listed as key/senior personnel (from here out: senior personnel) on a proposal to the federal funding agencies listed below must complete Research Security training within the 12 months prior to submission of a proposal:

- National Science Foundation (NSF)
- National Institutes of Health (NIH)
- Department of Energy (DOE)
- Department of Defense (DoD)

NIH specific

This training must be repeated by NIH awardees every 12 months.

In addition, prior to submission of an Other Support document, all senior personnel on a proposal to the National Institutes of Health must complete training on the requirements for disclosure of other support to ensure they fully understand their responsibilities.

Part II: Disclosures

- All senior personnel on a research proposal to or award from a federal funder must disclose to the funder and to Bates College any relationships or agreements with external organizations that are required by the funder on the Biographical Sketch and Current and Pending or Other Support document.

  ### NSF specific

  Senior personnel on NSF proposals must make disclosures as specified in the NSPM-33 Implementation Guidance Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support.

  ### NIH specific

  Senior personnel on NSF proposals must make disclosures as specified in the NIH Pre-award and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support.

  ### DOE specific

  Senior personnel on DOE proposals must disclose all Current and Pending Support, where this term has the same meaning as the term Other Support as applied to researchers in NSPM-33.

  ### NASA specific

  Senior personnel on NASA proposals must make disclosures as specified in the NASA Pre-award and Post-award Disclosure Requirements table.

- Senior personnel on federal proposals and awards must provide to Bates College supporting documentation, including copies of contracts, grants, or any other agreements that must be disclosed on the Biosketch and/or Current and Pending Support or Other Support documents. If the contracts, grants or other agreements are not in English, the individual must provide translated copies. Bates College will maintain any records for the record retention period of the project/award after which time they will be destroyed in accordance with Bates' Records Retention Policy, Records Retention Schedule, and Policy on Research Misconduct.

NSF specific

These agreements will be made available to the funding agency upon request from the funder.

Bates College will submit updated Current and Pending Support information to NSF within 30 days of discovery of any failure by senior personnel to disclose required Current and Pending Support information on a proposal.

NIH specific

Senior personnel must submit to NIH supporting documentation, including copies of contracts, grants, or any other agreements specific to senior/key personnel foreign appointments and/or employment with a foreign institution, and translated copies of all documents that are not in English, for all foreign activities and resources that are reported in Other Support.

Bates College will submit updated Other Support information to the Grants Management Specialist named in the Notice of Award as soon as any failure by a PI or other Senior/Key personnel on an active NIH grant to disclose Other Support information outside of Just-in-Time or the RPPR, as applicable, becomes known.

DOE specific

These agreements will be made available to the funding agency upon request from the funder.

NASA specific

Bates College will submit updated Current and Pending Support information to NSF within 30 days of discovery of any failure by senior personnel to disclose required Current and Pending Support information on a proposal.

Process/Responsibilities

Part I: Training

- All PIs, co-PIs, and individuals listed as senior personnel on a research proposal to NSF, DOE, DoD, or NIH must complete Research Security training within the 12 months prior to submission of a proposal. The College subscribes to online Research Security training courses through the CITI Program to assist in compliance. For access to the CITI program and instructions to enroll in this course.
    a. Go to https://www.citiprogram.org/login, then click on the REGISTER tab if you do not have an account already established. Follow the registration prompts to complete the account setup.
    b. Once logged in, click on the “Courses” page.
    c. Click on one of the “View Courses” links for the course listing of interest.
    d. Click on “Add a Course” which takes you to the course enrollment questions where your responses will add the Research Security Training course.
        i. The “Research Security Training (combined course) A condensed and combined single module course…” is sufficient to meet the training requirements.
    e. Click “Start Now” button on the Research Security Training module to begin your training
    f. Please email completed certificates and address any questions to the Office of Research and Sponsored Programs (orsp@bates.edu).

NIH specific

NIH awardees must complete/re-take Research Security training every 12 months for the life of their award.

Prior to submission of an Other Support document (typically during the JIT phase), senior personnel must review the NIH Pre-award and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support for NIH-specific disclosure requirements.

- The Research Integrity Officer will oversee compliance with Research Security Training requirements. The Office of Research and Sponsored Programs will assist the Research Integrity Officer by maintaining records of training and communicating training requirements to senior personnel, as needed.
- The Office of Research and Sponsored Programs will assist faculty with meeting requirements for submission of certifications of compliance to funders.

Part II: Disclosures

- Prior to proposal submission and any time an individual listed as senior personnel on an NSF, DOE, DoD, or NIH proposal or award enters into or modifies an agreement that must be reported on the Biosketch and/or Current and Pending Support or Other Support documents, the individual must complete the Bates College **Other Disclosures for Federal Funding form**.
    - Senior personnel must provide copies of all contracts, grants, agreements, etc that meet the threshold for inclusion on the Biographical Sketch and/or Current and Pending Support or Other Support documents.
    - English translation copies must be provided along with any documents that are not in English.
- The Office of Research and Sponsored Programs and the Research Integrity Officer will maintain disclosure records for the record retention period of the project/award, after which time the records will be destroyed.

NSF specific

ORSP will provide documentation of disclosures to NSF upon request, as required. ORSP will notify the senior personnel prior to providing documentation to NSF.

NIH specific

It is the responsibility of the senior personnel to include all required documentation of foreign agreements to NIH as part of their Other Support Disclosure.

DOE specific

ORSP will provide documentation of disclosures to DOE upon request, as required. ORSP will notify the senior personnel prior to providing documentation to DOE.

Policy owner

- Office of the Vice President for Academic Affairs and the Dean of the Faculty
    - Research Integrity Officer - Associate Dean Don Dearborn - researchintegrity@bates.edu

Contact

- Office of Research and Sponsored Programs - orsp@bates.edu

Last updated: 12/01/2025

Responsible and Ethical Conduct of Research

Principal Investigators are encouraged to review the College's institutional training plan for Responsible and Ethical Conduct of Research (pdf). Participation is mandatory for all PIs and senior personnel, students, and postdoctoral research associates on projects funded by the National Science Foundation. PIs on such projects are encouraged to use the resources detailed in this plan to devise their own project-specific plans. PIs on projects with other sources of external support are also encouraged to avail themselves of these resources in training students and others under their supervision.

The College subscribes to online training courses through the CITI Program to assist in compliance with Responsible Conduct of Research training. Please see below for access to the CITI program and instructions to enroll in this course.

1. Go to https://www.citiprogram.org/login, then click on the REGISTER tab if you do not have an account already established. Follow the registration prompts to complete the account setup.
2. Once logged in, click on the "Courses" page.
3. Click on one of the "View Courses" links for the course listing of interest.
4. Click on "Add a Course" which takes you to the course enrollment questions where your responses will add Responsible Conduct of Research (RCR) module
5. For undergraduate students and postdoctoral students, click "Students-RCR" and select the discipline that most aligns with your work (Biomedical, Social and Behavioral, Physical Science, or Humanities).
6. Click "Start Now" button on the RCR module to begin your training

Please email completed certificates and address any questions to the Office of Research and Sponsored Programs (orsp@bates.edu).

Last updated: 12/01/2025

Policy on Malign Foreign Talent Recruitment Programs

Effective Date: May 20, 2024

Purpose/Background

- This policy applies to proposers and recipients of funding from the National Science Foundation and the National Institutes of Health.
- This policy outlines Bates College's compliance with the requirements of the NSF Proposal and Awards Policies and Procedures Guide (PAPPG) and NIH Notice NOT-OD-25-154 regarding participation in Malign Foreign Talent Recruitment programs.

The National Science Foundation (NSF) and the National Institutes of Health (NIH) prohibit Individuals who are a current party to a Malign Foreign Talent Recruitment Program (MFTRP) from serving as a senior/key person on a proposal or on any award made after the effective date of each funder's respective policy (May 20, 2024 for NSF or September 11, 2025 for NIH). NSF and NIH require that:

1. At the proposal stage senior personnel certify that they are not party to a MFTRP,
2. An Authorized Organizational Representative certify that senior personnel have been made aware of their responsibilities to this effect, and
3. Individuals serving as a Principal Investigator (PI) or co-PI on an active award made on or after the effective date of the funders' policies certify annually to their participation or non-participation in an MFTRP.

Policy Statement

- Pursuant to Section 10632 (42 U.S.C. § 19232), each individual identified as senior/key person on an NSF or NIH grant must certify prior to proposal submission and annually thereafter for the duration of the award that they are not a party to a malign foreign talent recruitment program. False representations regarding this certification may be subject to prosecution and liability pursuant to, but not limited to, 18 U.S.C. §§.287, 1001, 1031 and 31 U.S.C. §§ 3729-3733 and 3802.

Definitions

The NSF Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 24-1) defines a Malign Foreign Talent Recruitment Program as:

> Any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to the targeted individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue, in exchange for the individual

1. engaging in the unauthorized transfer of intellectual property, materials, data products, or other nonpublic information owned by a United States entity or developed with a Federal research and development award to the government of a foreign country or an entity based in, funded by, or affiliated with a foreign country regardless of whether that government or entity provided support for the development of the intellectual property, materials, or data products;
2. being required to recruit trainees or researchers to enroll in such program, position, or activity;
3. establishing a laboratory or company, accepting a faculty position, or undertaking any other employment or appointment in a foreign country or with an entity based in, funded by, or affiliated with a foreign country if such activities are in violation of the standard terms and conditions of a Federal research and development award;
4. being unable to terminate the foreign talent recruitment program contract or agreement except in extraordinary circumstances;
5. through funding or effort related to the foreign talent recruitment program, being limited in the capacity to carry out a research and development award, or required to engage in work that would result in substantial overlap or duplication with a Federal research and development award;
6. being required to apply for and successfully receive funding from the sponsoring foreign government's funding agencies with the sponsoring foreign organization as the recipient;
7. being required to omit acknowledgment of the recipient organization with which the individual is affiliated, or the Federal research agency sponsoring the research and development award, contrary to the institutional policies or standard terms and conditions of the Federal research and development award;
8. being required to not disclose to the Federal research agency or employing organization, the participation of such individual in such program, position, or activity; or
9. having a conflict of interest or conflict of commitment contrary to the standard terms and conditions of the Federal research and development award. And
10. A program that is sponsored by—
    a. a foreign country of concern or an entity based in a foreign country of concern, whether or not directly sponsored by the foreign country of concern;
    b. an academic institution on the list developed under § 1286(c)(8) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. § 2358 note; Public Law 115–232); or
    c. a foreign talent recruitment program on the list developed under § 1286(c)(9) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. § 2358 note; Public Law 115–232).

The following are not considered malign foreign talent recruitment programs unless such activities are funded, organized, or managed by an academic institution or a foreign talent recruitment program on the lists developed under paragraphs (8) and (9) of section 1286(c) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 4001 note; Public Law 115–232):

1. making scholarly presentations and publishing written materials regarding scientific information not otherwise controlled under current law;
2. participation in international conferences or other inter- national exchanges, research projects or programs that involve open and reciprocal exchange of scientific information, and which are aimed at advancing international scientific understanding and not otherwise controlled under current law; and

3. advising a foreign student enrolled at an institution of higher education or writing a recommendation for such a student, at such student's request.

Process/Responsibilities

1. The Office of Research and Sponsored Programs will make all individuals identified as senior/key personnel on an NSF or NIH proposal aware of this policy and their responsibility to comply.
2. Senior/key personnel will certify compliance with this policy when downloading their biosketch from SciENcv.
3. Individuals serving as a Principal Investigator (PI) or co-PI on an active NSF or NIH award made on or after the effective date of the funders' policies must certify annually to their participation or non-participation in a MFTRP.
   a. NSF investigators certify in Research.gov
   b. NIH investigators upload a certification statement in Section G.1, Special Notice of Award and Funding Opportunity Announcement Reporting Requirements as a flattened PDF file. The file for each senior/key person must be named 'ResearchSecurities_[Name].pdf' without quotations, where '[Name]' is the name of the senior/key person.

Policy owner

- Office of the Vice President for Academic Affairs and the Dean of the Faculty
  - Research Integrity Officer - Associate Dean Don Dearborn - researchintegrity@bates.edu

Contact

- Office of Research and Sponsored Programs - orsp@bates.edu

Last updated: 12/01/2025

Policy on Export Control

Federal scrutiny of export control is an increasing concern in U.S. colleges and universities, and Bates is developing resources for faculty and staff to promote compliance. The two areas of export control are ITAR, administered by the State Department and governing military technologies, and EAR, administered by the Commerce Department, overseeing "dual use" and economically sensitive technologies. These policies apply to both information and equipment/technology.

All on-campus research at Bates is covered by the Fundamental Research Exemption. The export control regulations exempt from licensing requirements technical information (but not controlled items) resulting from "fundamental research." No license is required to disclose to foreign persons information that is "published and which is generally accessible or available to the public through fundamental research in science and engineering at universities where the resulting information is ordinarily published and shared broadly in the scientific community."

"Fundamental research" means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons. (National Security Decision Directive 189)

There are other areas of risk, however, when it comes to export control, particularly as they relate to "controlled items." Faculty travel involving technical data, technical reports, equipment, or technology to sanctioned countries is prohibited. We ask that faculty acquaint themselves with the countries that are subject to embargo. Travel to these countries may require consulting with ILS and the Director of Research and Scholarship about restrictions and possible exemptions. Please review Data Security and Technology Protection for International Travel. For example, taking a college laptop with standard software and no specialized data to certain embargoed countries is prohibited; the countries currently subject to sanctions for reasons of anti-terrorism are Cuba, Iran, North Korea, Sudan and Syria, although this list is subject to change. The Office of Foreign Assets Control (OFAC) provides information on sanctions for each of the above countries, as well as other OFAC-administered sanction programs. The OFAC website is at http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. Broader lists of countries may be subject to export control regimes covering certain controlled items, such as technical data not intended for publication or manuals to controlled equipment items. Faculty concerned about the security of data stored on their college laptop may wish to borrow a "clean laptop" from ILS for purposes of foreign travel. Please check with ILS about availability of such loaners as well in advance of your planned departure date as possible.

Embedded below is a link to a flow chart which is designed to assist faculty in determining if their research qualifies as exempt, or whether it may require referral to the DOF office for Export Control review: Export Control Decision Tree-Flow Chart

For those who require export control review, please complete and submit electronically a Travel Disclosure Form. If you believe your project requires an export control license or approval, please submit the form well

in advance of your travel dates.

In order to promote understanding of and compliance with the relevant Federal laws, we require that faculty traveling with college laptops or other equipment, complete the Export Control Overview module of CITI training available at https://www.citiprogram.org/index.cfm?pageID=93. The training is brief and summarizes federal export control regulations. Those working in science or engineering are encouraged to take the entire export control suite of CITI training modules.

In addition, we ask that faculty who intend to take college-owned equipment out of the country while employed at Bates complete a general Export Control Travel form_Sept. 2014 accepting the risks and personal responsibility for the decision to take college equipment abroad. According to federal guidelines, faculty are asked to:

- attend to export control guidelines,
- maintain effective control over the item,
- use secure internet connections,
- consult with the IT Service Desk at Bates College on firewall and encryption questions,
- utilize personal firewall protection and password protect any files that contain controlled technology, and
- ensure the device contains no mass market 64-bit encryption software or other encryption capabilities restricted under EAR.

These forms are available from the Director of Research and Scholarship and can be completed at any time and kept on file.

Last updated: 12/01/2025

Data Security and Technology Protection for International Travel

Owner: ILS

For members of the campus community, a trip to a foreign country presents unique data security challenges. The nature of international travel requires you to use your technology (laptop, tablet, or smartphone) in various unfamiliar places that may expose Bates' data and devices to malicious people and software. Following are a series of steps that you should take throughout your trip (before, during, and after) to safeguard your technology.

In addition to voluntary cybersecurity and technology protections, international travelers need to consider US export control laws and import restrictions imposed by the destination countries. Bates' Dean of Faculty Office has a website dedicated to export control that provides specific steps Faculty need to take prior to travel. US Export control laws are federal regulations that control the conditions under which certain information, technologies, and commodities can be transmitted overseas to anyone, including U.S. citizens, or to a foreign national on U.S. soil. Failure to comply with these laws can result in significant fines to you as an individual. Routine educational and research activities at Bates are generally exempt from export controls. If you have any questions about US Export control laws, please contact the Office of Research and Sponsored Programs at orsp@bates.edu.

If you have any questions about securing your data on your trip, please contact the Director of Information Security, Privacy, and Compliance at infosec@bates.edu.

BEFORE YOUR TRIP

1. Identify if the place you will be traveling to is defined as a "high risk" country by the U.S. Department of State as they issue current travel advisories and alerts that may affect your travel. The State Department establishes risk indicators based upon crime, terrorism, civil unrest, health, natural disaster, etc. While not specific to data security the State Department describes the risks and provides clear actions we should take to help ensure our safety. Follow the State Department's recommendation for whichever country you intend to visit.
    1. Beginning May 5, 2022 – If you are visiting any of the following countries/regions please contact the Support Desk so you can have your Duo account put into bypass mode – this will allow you to access Bates resources without needing to use Duo's Two-Factor Authentication.
        1. Cuba
        2. North Korea
        3. Iran
        4. Sudan
        5. Syria

6. Crimea region
7. Sevastopol region
8. Donetsk region
9. Luhansk region

2. The following nations restrict the import of encrypted devices and do not recognize a “personal use exemption”. A group of nations negotiated a set of rules attempting to facilitate traveling with encryption software known as the “Wassenaar Arrangement.” One of its provisions allows a traveler to freely enter a participating country with an encrypted device under a “personal use exemption” as long as the traveler does not create, enhance, share, sell or otherwise distribute the encryption technology while visiting. In general, low-risk countries, e.g., the EU, Australia, and Canada are safe. If traveling to one of the following countries, it is best to leave your laptop home and consult with the Bates IT Service Desk to borrow a loaner laptop for your trip.

Belarus	Hungary	Morocco	Sudan
Burma (Myanmar)	Iran	North Korea	Syria
China	Kazakhstan	Russia	Ukraine
Cuba	Moldova	Saudi Arabia	

3. Regardless of where you are going abroad, be sure your Bates laptop is configured with Bates’ VPN software. Using the VPN will allow you to access campus resources (e.g., campus network drives, Banner). Consult with Bates IT Service Desk for assistance.
4. Backup your data. Whether you are traveling with a loaner computer, your regular computer, tablet, or smartphone, you should always backup your data. Consider moving your documents pertaining to Bates to a College-provided folder (i.e., Google Drive) that you can access remotely instead of carrying these files on your local device(s).

DURING YOUR TRIP

1. Do NOT leave your device unattended, especially in your checked bag on your flight. If you ever leave your computer, make sure to turn it off completely instead of just hibernating it or putting it to sleep. When the computer is off, it is fully encrypted.
2. Connect only to known wifi networks. Anyone can create a network and give the network a legitimate-sounding name, hoping to lure unsuspecting travelers to connect while capturing personal information transmitted through the network. This is especially prevalent at public cafes, hotel lobbies, and airports. When connecting to a network, find out the correct network name from the staff at the business and connect to it.

3. Use EDUROAM where available. It provides easy, secure connectivity from thousands of hotspots across more than 100 countries. Eduroam (education roaming) is the secure, worldwide roaming access service developed for the international research and education community. Eduroam allows students, researchers, and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions.
4. Turn off your wifi when not in use. Attackers can easily spoof Wifi network names to connect to devices within range for eavesdropping. To help you avoid accidentally connecting your device to rogue wifi networks at a later time, once you are finished using the network, turn off wifi on your device.
5. Do NOT enter your credentials into public computers. Public computers such as hotel business center workstations and internet cafe computers are often poorly managed and provide minimal security protection for their users.
6. US Customs and Border Protection may request that you be subject to an inspection of your electronic devices for a variety of reasons. Please review their Quick Reference to familiarize yourself with the process.

UPON YOUR RETURN HOME

- Upon returning home and returning your loaner device, change any passwords you used while you were traveling. Use a trusted computer, whether it's your own or one provided by the IT support staff, to reset credentials that were used during the trip. For example, if you use your Bates credentials during the trip, go to the Bates IT Service Desk website to reset your Bates password.