



CSUB Federal Research Security Training (RST) Procedures

Overview

To comply with emerging federal mandates, institutions must ensure that covered individuals involved in federally funded research complete appropriate Research Security Training (RST). This guidance outlines training available that aligns with requirements from the CHIPS and Science Act of 2022, NSPM-33, and federal funding agency directives from the Department of Energy (DOE), National Science Foundation (NSF), National Institutes of Health (NIH), Department of Defense (DOD) and others. Information on the Act can be found at [CHIPS and Science Act](#).

The training is required for any individual who contributes in a substantive, meaningful way to the development or execution of the scope of work on a federally funded research project. This includes, but is not limited to, Principal Investigators (PIs), Project Directors (PDs), and co-investigators. For some applications and projects this training must be completed prior to the submission of a proposal application to the agency.

Securing the nation's research enterprise is part of the mission of all federal funding agencies. Specifically, NSF works closely on this effort with its funding agency counterparts and with the law enforcement and intelligence communities — consistently emphasizing the importance of balancing research security with international collaboration in science and engineering. NSF has taken the lead in developing training modules that will meet the requirements of the Research Security Training (RST).

Additionally, NIH requires recipients to provide training to all faculty and researchers identified as [Senior/Key Personnel](#) on the requirement to disclose all research activities and affiliations (active and pending) in Other Support (see [Other Support form](#)). This requirement to train researchers to comply with other support disclosure requirements adds to the current policy (see NIH Grants Policy Statement (GPS), [Section 2.5.1 "Just-in-Time Procedures"](#)) in order to provide a comprehensive plan in the area of disclosure requirements for recipients. See [NIH Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements](#) for more information.

Research Security Training (RST) Program

The Research Security Training (RST) consists of 4 modules taking approximately 1 hour each to complete for a total of 4 hours training time including the topics below:

- **Module 1:** What is Research Security? Learn key concepts of research security and how to recognize situations that may indicate undue foreign influence. Understand the regulatory landscape that shapes research security and discover what you can do to safeguard the core values that underpin U.S. academic research.
- **Module 2:** Disclosure. Learn about federal funding agency disclosure requirements, including types of information that must be disclosed, how that information is used, and



why such disclosures are fundamental to safeguarding the U.S. research enterprise from foreign government interference and exploitation.

- **Module 3: Manage and Mitigate Risk.** Learn to identify types of international collaborative research and professional activities, associated potential risks, and strategies and best practices for managing and mitigating such risks. Learner experience will be customized based on their role as either a researcher or administrator.
- **Module 4: International Collaboration.** Learn about the role of principled international collaboration in U.S. science, innovation, and economic competitiveness. Discover how to balance principled international collaboration with research security concerns and foster an open, welcoming research environment that fulfills research security needs.

Research Security Training (RST) Program Procedures

- The 4 training modules are accessed through the NSF website here: [NSF Research Security Training](#).
- Because NSF will NOT maintain the training records in their database, after completing each module a certificate will be provided.
- You will generate a certificate of completion by typing your name and date in the certificate and save a copy as a PDF, or by taking a screen shot of the certificate.
- Once completed, you must send a copy to Gwen Parnell, Research Compliance Analyst in the GRaSP office.
- The GRaSP office will be responsible to the federal agencies for reporting purposes.
- The training must be completed on an annual basis. Any new PI(s) or Co-PI(s) added to an existing or ongoing project must complete the training within 30 days.

Revised on September 9, 2025