Office of the Vice President for Research

March 2024

DISCUSSION GUIDE ON

Research Security and Compliance

Notes for MIT principal investigators to support informational conversations with research groups and advisees

This document is intended to contribute to awareness of key principles underlying research security and compliance affecting research groups at MIT.

Specifically, these notes aim to support and guide you, as a principal investigator (PI), in approaching an educational conversation on these topics with your research group. Such dialogues can be helpful in avoiding misconceptions and can foster ongoing, open discussion of norms and expectations in the group. (In these notes, the word *group* refers to the research group; the guidance also applies to conversations with individual advisees.) This is particularly important in light of the U.S. government's growing focus on research security in universities and research institutes.

This document may be adapted for use across the Schools and the College of Computing; however, please note that the principles and related policies apply to every individual and unit engaging in research at MIT. Should you have questions, please contact research-compliance-help@mit.edu.

Suggested Overview

- Our group works to carry out world-class fundamental research that will be shareable with our peers and the global public, as appropriate.
- At the same time, we need to be aware of and follow good research security and compliance practices. This is our responsibility by virtue of working within the U.S., at MIT, and with the support of our sponsors.
- What do we mean by **research security**? The U.S. government defines it as "safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference."
- What do we mean by **research integrity**? The U.S. government defines it as "the use of honest and verifiable methods in proposing, performing, and evaluating research; reporting research results with particular attention to adherence to rules, regulations, guidelines, and following commonly accepted professional codes or norms."
- Our group works hard and takes pride in our research and its potential for positive impact on society. If we have a clear-eyed view of the risks we face and if we are aware of where we can get assistance, we can do our best work in a confident manner.
- Our colleagues in Research Administration Services, Research Compliance, the Environment, Health & Safety Office, and other support groups at MIT provide key guidance and rules that are aligned with MIT's mission and core values. We should invest the effort to follow prudent and commonsense practices.

Key Compliance Requirements

Transparent Reporting

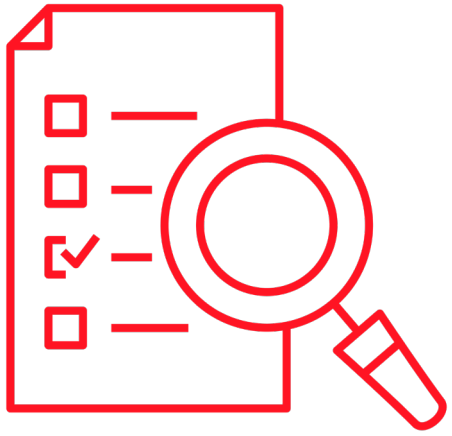
- To guard against undue external influence, the U.S. government imposes mandatory disclosure and reporting requirements on federally funded projects. It's crucial that we record the time spent working on federally funded efforts in a timely and accurate way. Those considered to be in key roles must also accurately report to government sponsors concerning any outside financial interests and professional commitments.
- Separately, and regardless of the source of funding for our research, including gifts provided to support research, MIT policy requires each of us to report to the Institute any personal financial interests or outside professional activities that have the potential to pose a conflict of interest or conflict of commitment to our responsibilities here.
- Remember that our internal processes for reporting to MIT are separate and distinct from reporting to the government sponsors of our research. It is important to make sure that what we each report to MIT and to sponsors is **transparent, complete, and consistent**. Discrepancies in reporting can cause serious problems.

Export Controls

- Engagements with colleagues outside the U.S. are subject to export control laws. Before sending any materials (including tangible items such as prototypes, technology, and software) outside the U.S., which could inadvertently violate export control laws, we need to check with MIT's Export Control Team. *(If your research group has a Technology Control Plan, discuss the plan's specific requirements.)*
- Some research institutions outside the U.S., including universities, are subject to country-specific or institution-specific sanctions. We must check with the Export Control Team to assure that no such sanctions apply to our collaborators. This can be coordinated through the Director of Administration & Finance or other administrative officer for our DLCI. More generally, any of us can use MIT's Informal International Collaborations tool to learn whether there may be concerns about an individual collaborator or their institution.
- Some agreements specifically call out restrictions on exports. Export Control can assist your understanding of any such agreement-specific restrictions.

Cyber Security

- Our work needs to be kept secure from cyber threats that can derail our research and cause significant damage. Use good cyber hygiene practices. Embrace two-factor authentication. Use unique passwords and change them when asked to do so. If you're not familiar with these tools and concepts, please take IS&T's quick training.
- If you see something that looks odd in a system, tell the administrator or your PI. Do not delay. Cyber intrusions can seem like small anomalies but, left unaddressed, can have large consequences. Do not let the pressure of time or doubt keep you from taking appropriate action to protect yourself, the research group, and MIT.



International Travel

- If you travel internationally, whether for personal or professional reasons, you need to be familiar with the best ways to protect yourself and your electronic assets when traveling abroad.
- MIT has **international travel guidance** covering these topics. When traveling on behalf of MIT, **MIT's International Travel Risk Policy** requires that you **register your travel** with MIT for your safety and well-being.

Working Outside the Research Group

- As MIT researchers, our skills and knowledge are in high demand. If you have any work going on outside of our research group, it's very important to keep an open line of communication with your PI about the work you're performing and its relationship (if any) to what we're doing here. It is imperative that we not let conflicts develop between the research group's work and external efforts. Conflicts may be:
  - A financial conflict of interest, where two or more obligations run counter to each other.
  - A conflict of commitment, where a researcher has a time commitment exceeding 40 hours per week (or other maximum pursuant to their visa status) or 100% employment.
- If you find yourself potentially conflicted in either of these ways, tell your PI or supervisor.
- If presented with an opportunity to pursue work outside the research group, fill out the **COI Consulting Questionnaire**.
- Members of the MIT community have varying academic commitments and privileges based on employment status, and the opportunities and requirements vary.

Using Available MIT Resources

None of us is expected to have all the answers when it comes to research security practices. Fortunately, we have resources available, including those identified above.

- MIT provides online **peer-reviewed training courses** on a range of research security topics, including those we've discussed.
- MIT's Office of the Vice President for Research, the Office of the Vice Provost for International Activities, the Office of the General Counsel, and other offices can help.
- Rather than trying to figure out who can best help solve specific research compliance and security questions, you can email **research-compliance-help@mit.edu** to get directed to the appropriate resource.
- **Community COI Portal**
- **COI Policy** and **Outside Professional Activities Policy**
- **Guidance on Outside Professional Activities**
- **Guidance on Foreign Engagement**
- **Global Support Resources**
- **International Travel Risk Policy**
- **Securing Computers and Mobile Devices**
- **Export Control**