

Security First: Safeguarding Research in Funding Applications

October 6, 2025

Case Study

Professor (Prof.) F., a researcher in the Department of Electrical & Computer Engineering (ECE) at the Faculty of Applied Science & Engineering (FASE), would like to apply for a new NSERC (Natural Sciences & Engineering Research Council) Alliance funding opportunity for a project to develop improvements to the micro-electromechanical system (MEMS) temperature sensors in air conditioning systems. Microelectronics are identified as sensitive, per the Canadian government's Sensitive Technology Research Areas (STRA) list, because it may be of interest to external actors due to its dual use capabilities.

Prof. F will be the lead Principal Investigator (PI) on the application. The co-applicant is Prof. Q, another researcher at FASE ECE, who recently published research on MEMS accelerometers in partnership with Prof. H at National University of Defense Technology (NUDT). Prof. F would like to have two PhD students participate in the research as highly qualified personnel (HQPs), including a visiting student from Tsinghua University.

The research will also include a corporate partner, *Room Temp HVAC*, a Toronto-based HVAC systems company with a subsidiary in Berlin and manufacturing plants in India, China, Malaysia, and the US. Room Temp will have four co-investigators from the company participate in the research and will supply some of the materials.

The research will take place at both Room Temp's research and development centre and Prof. F's lab, with participants accessing both locations on a routine basis over the duration of the project. Prof. F and Room Temp have signed agreements concerning publication, intellectual property (IP) usage, and patents.

1. Which federal research security processes apply in this case? What key documents and policies would you recommend Prof. F to become familiar with?
2. Are there any affiliations of concern that could prevent this project from receiving funding?
3. What are some risk mitigators that Prof. F should consider putting in place to ensure the security of the research?
4. If Prof. F wanted to apply for an Ontario grant, what processes and policies would apply, if any?

Scan the QR code to access the Research Security Self-Assessment Tool or find it at <https://research.utoronto.ca/safeguarding-research/research-security-self-assessment>



Case Study Answers

Answer 1:

As this research proposes to advance a sensitive technology, the policy on Sensitive Technology Research and Affiliations of Concern (STRAC) applies. This means that all named academic researchers on the proposal, including applicants from international institutions, must complete an individual attestation form that they do not have any affiliations to any research organizations identified on the Canadian government's Named Research Organizations (NRO) list at the time of application and for the duration of the grant. HQPs are not required to submit an attestation form; however, they are required to comply with the STRAC policy for the duration of the grant.

In addition, because this proposal includes a corporate partner, NSERC Alliance (and some other Tri-Agency grants) will apply the National Security Guidelines for Research Partnerships (NSGRP). This means the lead PI (Prof. F) will need to complete the NSGRP Risk Assessment Form (RAF). One RAF is required for the whole project, regardless of the number of corporate partners. Under NSGRP, the funding agency reviews the corporate partner and associated co-investigators for any security risks and considers a broader range of entities and factors than the STRAC process. This could include, but is not limited to, a review of the corporate partner's management; the structure, including subsidiaries; who has beneficial / controlling ownership; and corporate partners. Individuals affiliated with the corporate partner are not required to complete an attestation form as their participation is governed by the NSGRP process, not the STRAC process.

Answer 2:

- Prof. F does not have any known affiliations of concern.
- Prof. Q recently published research with an entity on the NRO list. As such, Prof. Q must ensure that the research partnership with NUDT has ended. If the partnership has concluded, Prof. Q has no affiliations of concern. If the partnership has not concluded and Prof. Q continues to engage in research with NUDT or is actively working to publish more work with NUDT, then Prof. Q has an affiliation of concern, making Prof. Q ineligible to participate in Prof. F's research project until such time as Prof. Q's affiliation to NUDT has ended.
- Any HQP who is a full-time student at U of T is affiliated with U of T, regardless of where they previously studied (so long as they are not actively engaging in research with or employed by their former institution if it is on the NRO list).
- Visiting students remain affiliated with their home institutions for the duration of their time at U of T. In this case, Tsinghua University is not on the NRO list, so the visiting student is eligible to participate in Prof. F's research.

Answer 3:

Risk mitigators include but are not limited to:

- If data from the project is being stored digitally, Prof. F will want to ensure that data security and cybersecurity measures are in place. If the corporate employees have access to the data, will it be accessed remotely? Will it be password protected?

- Since individuals external to the University, namely Room Temp's employees, will have access to U of T labs, Prof. F will want to consider how access is granted to these individuals and to what extent. For example, are they granted swipe keys? Are they required to be accompanied by lab staff at all times?
- Prof. F will want to ensure an understanding of how Room Temp shares information with its subsidiaries and manufacturing plants / partners to determine Prof. F's level of comfort with that arrangement. Prof. F may decide to add clauses to the partnership contract addressing any concerns that arise (the Innovation and Partnership Office assists with contracts).

Answer 4:

If Prof. F wanted to apply for an Ontario grant, Prof. F will need to complete the Mitigating Economic and Geopolitical Risk checklist as well as an Application Attestation Form.

Resources

Contact the Research Security Team (RST) at any point in the application process for assistance conducting partner due diligence and help with completing any required research security paperwork. PIs are encouraged to contact the RST as early as possible in their partnership development process.

- Research Security inbox: researchsecurity@utoronto.ca
- Research Security webpage: <https://research.utoronto.ca/safeguarding-research/safeguarding-research>
- Safeguarding Your Research Portal: <https://science.gc.ca/site/science/en/safeguarding-your-research>
- STRAC Policy: <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern>
- NSGRP Policy: <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships>
- Tri-Agency Guidance on STRAC: https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/strac-rtsap_eng.asp
- Tri-Agency Guidance on NSGRP: https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_eng.asp
- CFI Research Security: <https://www.innovation.ca/apply-manage-awards/resources-apply-manage-award/research-security>
- Research Security Guidelines for Ontario Research Funding Programs: <https://research.utoronto.ca/sites/default/files/2024-06/Research%20Security%20Guidelines%20and%20FAQs.pdf>