

To: Stanford Faculty and Staff
From: Ann Arvin, Vice Provost and Dean of Research
Date: March 30, 2016
Re: Memorandum on Relationships with Entities Identified as Presenting Elevated Export Control or Information Security Risks

This memo addresses steps that must be taken by Stanford faculty in advance of initiating a research collaboration, industrial affiliate relationship, or other institutional research relationship with an entity (“Entity”) that the Dean of Research (DoR) office, together with the Information Security Office has determined presents elevated export control or information security risks. The Export Control Officer, the Industrial Contracts Office and the Office of Sponsored Research will assist Faculty in identifying such Entities. The determination of risk will be based on US Government Restricted Party List screening, information provided to the University by a federal agency, or information in the public domain.

In some cases, the finding may be that it is unlawful to engage with an Entity. If it is not unlawful, but risks are identified, the faculty member who is responsible for the research-related activities with the Entity, either as a PI, industrial affiliates program director or in another role under the terms of the University’s agreement with the Entity must:

1. Inform the School Dean, the Export Control Officer and the Information Security Officer in advance and in writing of onsite activities proposed for visitors from the Entity. In some cases, a plan may be required to supervise those visitors working with Stanford research groups when they are on campus.
2. Meet with the Export Control Officer to discuss potential export control risks, and the process for review by the Export Control Officer of visitors from the Entity who will be working on campus.
3. Obtain approval from the Information Security Office before allowing representatives of the Entity to transport, install or otherwise implement hardware or software on campus.
4. Ensure that representatives of the Entity are not issued a SUNet ID.

There may be instances when the Export Control Officer and the Information Security Officer determine in collaboration with a non-academic unit that the non-academic unit’s proposed business relationship with an Entity presents elevated export control or information security risks. In those instances, the non-academic unit will be expected to implement Steps 1-4 above.

General questions regarding this policy should be addressed to Steve Eisner, Export Control Officer (steve.eisner@stanford.edu, 724-7072). Specific questions regarding information security procedures should be addressed to Michael Duff, Assistant Vice President and Chief Information Security Officer (securityofficer@stanford.edu, 721-3111).