Brookhaven National Laboratory

Super Intelligence (SI)
Export Control - Quick Reference Guide

Purpose: This Quick Reference Guide provides a rapid screening tool to help identify when SI activities may require export control review. This guide does not authorize any export activity and is not a substitute for formal Export Control review. For detailed ECCN classification guidance, refer to the *SI – ECCN Classification and Determination Guide*. For broader export-control risks and regulatory considerations, refer to the *SI – Export Control Guidance and Risk Considerations*. For Genesis-specific activities, refer to the *SI – Export Control Genesis Implementation Guide*.

What you need to know

SI work can raise export-control concerns even when nothing is shipped, the work is internal, or the research is ongoing. Risk may depend on access, collaboration, system capability, performance, scale, end use, end user, and destination.

Not all SI activities are controlled. General administrative SI use, public-domain tools, and research intended for full public release are typically lower risk. “Public” means fully and legally available without access restrictions, sponsor limits, approval requirements, or other controls. Posting material on GitHub or similar platforms does not automatically make it public if any access restriction exists. However, non-public models, model weights/parameters, source code, datasets, advanced computing resources, or sensitive applications may require review.

What counts as an export

An export may include sharing SI models, model weights/parameters, source code, software, technical information, or datasets with non-U.S. persons. A “non-U.S. person” refers to an individual who is not a U.S. citizen, lawful permanent resident, or protected individual under U.S. immigration law.

Providing access to systems, repositories, cloud or high-performance computing environments, or collaborative platforms may also constitute an export, including when access occurs within the United States. Remote access from outside the U.S. is treated as an export to the country where the user is located.

Quick Risk Check - Contact Export Control if the activity involves:

- Foreign collaborators or non-U.S. person access.
- Non-public SI models, model weights/parameters, source code, or datasets.
- High-performance, shared, cloud-based, or externally hosted computing environments.
- SI applications involving cybersecurity, surveillance, energy systems, advanced materials, microelectronics, chemical/biological applications, autonomous systems, or other sensitive uses
- Advanced or high-capability SI models. Examples may include large language models (LLMs), advanced generative models, or models trained using substantial high-performance computing resources.
- SI systems operating in autonomous or closed-loop environments.

Note: Export control regulations are subject to change. Refer to the current applicable regulations and agency guidance.

- Large-scale or multi-institution collaborations.
- Unclear end use, end user, destination, access level, publication status, or classification.
- Involvement of sanctioned or embargoed countries
- Collaboration with or access by restricted or denied parties

If yes or unsure, contact Export Control before proceeding.

Quick Risk Indicator

🟢 **Green: Lower Risk – Awareness Required**

Examples:

- General administrative or non-technical SI use
- Fundamental research intended for full public release
- Publicly available tools or data with no restricted access or sensitive end use

🟡 **Yellow: Moderate Risk – Contact Export Control**

Examples:

- Use of non-public data
- Collaboration with foreign institutions
- Sharing code, models, datasets, or technical information not clearly public
- Use of shared, cloud-based, or high-performance computing resources
- Foreign-person access to internal SI systems or repositories

🔴 **Red: High Risk – Contact Export Control Before Proceeding**

Examples:

- Non-public model weights/parameters
- Training or fine-tuning using advanced computing resources
- Providing system, repository, cloud, or administrative access to foreign persons
- SI applied to cybersecurity, surveillance, chemical/biological, advanced materials, microelectronics, energy infrastructure, or other sensitive applications
- SI systems used in autonomous or closed-loop control of physical or experimental systems
- Any activity involving sanctioned countries or restricted parties

Common misconceptions

- ❖ Research is not always uncontrolled
- ❖ GitHub does not always mean public
- ❖ Internal access can still be an export
- ❖ Software and data can be controlled
- ❖ EAR99 does not mean no restrictions
- ❖ Fundamental research status applies only to resulting information that is ordinarily published and shared broadly. It does not apply to restricted inputs, controlled software, non-public datasets, model weights/parameters, or access-controlled systems.

EAR99:

Items classified as EAR99 may still require restrictions or review based on end use, end user, destination, sanctions, restricted parties, or other regulatory concerns.
ECCN classification, including EAR99, does not by itself determine whether an activity is permitted.

When to Contact Export Control:

Contact the Export Control Office before sharing with foreign persons, using high-performance or shared computing environments, working with non-public models, model weights/parameters, source code, or datasets, collaborating with external or foreign institutions, or when unsure.

Certain activities may require a U.S. Government export license, license exception review, access controls, or may be prohibited depending on the end use, end user, destination, sanctions, and classification.
Contact: BNL Export Control Office: export@bnl.gov

Note: Export control regulations are subject to change. Refer to the current applicable regulations and agency guidance.