Brookhaven National Laboratory

Super Intelligence (SI)
Export Control – Genesis Implementation Guide

Purpose: This document provides program-specific guidance for applying BNL SI Export Control requirements within the Genesis initiative.

Genesis is a shared, collaborative scientific-computing and SI environment supporting multi-institution research and advanced system integration.

This document should be used in conjunction with the *SI – Export Control Quick Reference Guide*, *SI – Export Control Guidance and Risk Considerations*, and *SI – ECCN Classification and Determination Guide*, as applicable.

Scope:

This guidance applies to Genesis participants, including researchers, staff, collaborators, and system users working with:

- SI models, including model weights/parameters
- Training data and datasets
- Source code and software
- Computing environments, including on-premise, shared, cloud-based, or high-performance computing resources
- SI-enabled systems integrated with scientific infrastructure, experimental platforms, or physical systems

Shared and multi-user infrastructure can increase the risk that non-public data, models, or system capabilities are exposed without proper access review.

Genesis activities should be reviewed when they involve non-public SI models, model weights/parameters, source code, restricted datasets, advanced computing resources, externally hosted platforms, foreign-person access, external collaborators, or SI-enabled interaction with physical, cyber, energy, scientific, or infrastructure systems.

Regulatory Scope:

In addition to the Export Administration Regulations (EAR), Genesis activities must comply with U.S. sanctions programs administered by the Office of Foreign Assets Control (OFAC). Certain countries, entities, and individuals may be subject to comprehensive or targeted sanctions that prohibit access or collaboration regardless of export classification.

Key Risk Areas in Genesis

Genesis involves shared infrastructure, advanced SI capabilities, and collaborative environments that may increase export control and national security risk.

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

Particular attention should be given to:

- Foreign-person access to systems, models, or non-public data
- Use of shared, high-performance, cloud-based, or externally hosted computing environments
- Storage or sharing of non-public SI models, model weights/parameters, source code, or datasets
- Collaboration with external institutions, foreign institutions, industry partners, or multi-institution teams
- SI applications involving cybersecurity, surveillance, advanced materials, microelectronics, chemical/biological applications, energy systems, or other sensitive use cases
- SI-enabled control, optimization, or interaction with physical systems, including experimental infrastructure, energy systems, particle accelerators, or real-time decision-making systems
- Use of large-scale or aggregated datasets where sensitivity may arise from source, context, scale, or application
- Development or use of advanced or high-capability SI models
- Repository, API, administrative, system-level, training, fine-tuning, or download access that may reveal non-public models, source code, model weights/parameters, datasets, or controlled technical information

Closed-Loop and Autonomous SI Systems

Closed-loop or autonomous SI systems are escalation triggers. Contact Export Control before enabling SI outputs to directly control or materially influence physical systems, experimental processes, infrastructure, cyber systems, energy systems, safety-relevant systems, or real-time operational decisions.

Required User Actions

Genesis users must not share, upload, release, publish, transfer, or provide access to non-public SI models, model weights/parameters, source code, technical data, restricted datasets, or controlled computing environments until export control review has been completed where required.

Controls may include Technology Control Plans, access restrictions, role-based permissions, user authentication, logging, and data segregation.

Genesis users must:

1. Perform Initial Screening:
   Use the ***SI Export Control Quick Reference Guide*** before starting, sharing, or providing access to SI-related materials.
2. Evaluate Access:
   Confirm whether any non-U.S. persons will have access to systems, computing environments, models, model weights/parameters, source code, non-public datasets, or technical information. Confirm that all external collaborators, institutions, and users have been screened against applicable U.S. government restricted party lists prior to granting access.
3. Assess Work Activities
   Identify whether the work involves shared or high-performance computing, non-public or export-sensitive SI capabilities, integration with physical systems, sensitive applications, or collaboration with foreign entities or external partners.
4. Pause and Escalate When Needed:
   Contact the Export Control Office before proceeding if access, classification, end use, end user, destination, publication status, or sensitivity is unclear.
5. Ensure Compliance Controls:
   Confirm that access to systems, models, datasets, and computing environments is controlled and documented in accordance with export-control and institutional requirements.

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

Access and Collaboration Controls

Access to systems, platforms, models, datasets, repositories, or computing environments must be evaluated before permissions are granted to non-U.S. persons.

Access decisions must consider destination, end use, end user, and applicable sanctions restrictions. Access from outside the United States is treated as an export to that country.

Sharing non-public SI models, model weights/parameters, datasets, source code, or technical information must be reviewed for export control implications.

Collaborations with external institutions or industry partners should include export control screening and evaluation of data, model, system, and platform access.

Externally hosted, cloud-based, or multi-user platforms should be assessed to ensure appropriate control of access and information exposure.

Deemed Export Considerations

Providing foreign persons, including employees, researchers, collaborators, students, visitors, or contractors in the United States, with access to controlled SI systems, models, software, source code, model weights/parameters, datasets, or technical information may constitute a deemed export. Deemed export licensing requirements may apply depending on the nationality of the foreign person and the classification of the technology.

This may include access through:

- Shared platforms, repositories, or collaborative environments
- Model training or fine-tuning systems
- Cloud-based, high-performance, or externally hosted SI environments
- Interactive systems where underlying capabilities can be learned, inferred, extracted, or replicated

When to Contact Export Control

Contact the BNL Export Control Office before proceeding with Genesis activities involving:

- Foreign collaborators, users, or foreign-person access
- Non-public SI models, model weights/parameters, source code, datasets, or technical information
- High-performance, shared, cloud-based, or externally hosted computing environments
- SI applications tied to sensitive infrastructure, cybersecurity, surveillance, autonomous or closed-loop operations, advanced scientific systems, energy systems, advanced materials, microelectronics, or chemical/biological applications
- Unclear end use, end user, destination, access level, publication status, or classification
- Activities involving sanctioned or embargoed countries, or potential matches to restricted party lists.

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: export@bnl.gov

Relationship to BNL SI Export Control Guidance

- Use the *SI – ECCN Classification and Determination Guide* for detailed ECCN classification guidance.
- Use the *SI – Export Control Guidance and Risk Considerations* for broader export-control risks and regulatory considerations.
- Use the *SI – Export Control Quick Reference Guide* for initial risk screening.
- Use this document for Genesis-specific export-control implementation and requirements.

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