Brookhaven National Laboratory

FOCUS:
Super Intelligence (SI)

Export Control Guidance and Risk Considerations

Purpose

This document provides guidance to help BNL researchers and staff identify and understand export-control risks associated with Super Intelligence (SI) technologies, systems, software, and related technical information. It addresses key considerations, including foreign-person access, deemed exports, international collaborations, restricted parties, sensitive applications, and access to SI models, datasets, and computing environments. The guidance is intended to help recognize activities that may require additional review and consultation with the Export Control Office.

How to Use This Document: Use this guide to understand broader export-control risks associated with SI technologies, including foreign-person access, deemed exports, international collaboration, restricted parties, and sensitive applications. For detailed ECCN classification guidance, refer to the *SI – ECCN Classification and Determination Guide*. For initial risk screening, use the *SI – Export Control Quick Reference Guide*. For Genesis-specific activities, refer to the *SI – Export Control Genesis Implementation Guide*.

Regulatory Note: *Export controls related to super intelligence are rapidly evolving. Classifications and licensing requirements should be periodically reassessed to ensure alignment with current U.S. government regulations and policies.*

Recent U.S. policy initiatives related to super intelligence may influence agency priorities, but classification and licensing determinations must be based on the EAR and BIS regulations.

ITAR Disclaimer: *This document applies only to Super Intelligence technologies, subject to the Export Administration Regulations (EAR). If the SI system, software, data, or application may be subject to the International Traffic in Arms Regulations (ITAR), STOP and consult the Export Control Office immediately before any access, use or transfer, or release.*

Examples that may require ITAR review include SI used for military targeting, weapons integration, defense-specific autonomous systems, military sensor fusion, or other defense-specific applications.

What's Controlled? – The Big Picture

SI technologies are dual-use. They support civilian and research applications such as healthcare, energy systems, climate modeling, and scientific discovery, but may also support military, intelligence, cybersecurity, surveillance, energy security, or other national-security applications.

Export-control risk may involve:

- Hardware, including specialized SI chips, accelerators, and high-performance computing systems
- Software, including SI/ML models, training frameworks, inference tools, and source code
- Technology, including algorithms, model architectures, training methods, documentation, and technical information
- Datasets, including non-public, proprietary, sponsor-restricted, or controlled technical data
- Access to models, model weights/parameters, computing environments, repositories, cloud platforms, or collaborative systems

Not all SI activities are controlled. Public-domain tools, general administrative SI use, and research results intended for full public release are typically lower risk. Risk increases when the work involves non-public information, sensitive applications, foreign-person access, advanced computing resources, restricted parties, or unclear end use/end user.

Sanctions and Restricted Party Controls

Export control compliance includes U.S. sanctions programs administered by the Office of Foreign Assets Control (OFAC). Certain countries, entities, and individuals are subject to comprehensive or targeted sanctions that may prohibit exports, access, or collaboration regardless of ECCN classification.

All external collaborators, institutions, and users must be screened against U.S. government restricted party lists (e.g., Entity List, Denied Persons List, SDN List) prior to sharing non-public materials or granting access.

ECCN Determination – General Approach

ECCN classification depends on the item, software, technology, function, performance, design intent, end use, and end user.

Link to EAR Commerce Control List (CCL): https://www.bis.gov/ccl-index

Common CCL categories relevant to SI may include:

Category 3: Electronics and advanced computing hardware
Category 4: Computers, high-performance computing, and related software/technology
Category 5: Telecommunications and information security

General steps:

1. Confirm the item's purpose and design intent
2. Evaluate performance, capability, scale and function
3. Determine whether the item is specially designed for a controlled application
4. Identify potentially applicable ECCN categories
5. Assess end use, end user, destination and restricted-party concerns
6. Consult Export Control if classification is unclear.

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

Deemed Exports

Providing foreign persons, including employees, researchers, collaborators, or visitors in the United States, access to controlled SI models, software, source code, model weights/parameters, datasets, or technical information may constitute a deemed export.

This may include access to shared repositories, cloud platforms, training environments, fine-tuning systems, or interactive systems where controlled capabilities can be learned, inferred, extracted, or replicated.

KEY SI Areas of Concern

SI Compute and Hardware

Advanced computing systems used for large-scale SI training or processing may be controlled based on performance, configuration, destination, end use, and end user. Certain integrated circuits and related systems may fall under ECCNs such as 3A090 and 4A090, while other computing systems may be controlled under ECCN 4A005 or other applicable ECCNs depending on configuration and performance.

In addition to hardware classification, restrictions may apply under Part 744 end-use and end-user controls even when hardware thresholds are not exceeded.

SI Models, Software, and Model Weights/Parameters

SI software and models may raise export-control concerns when designed or used for:

- Military, intelligence, or surveillance applications
- Cyber operations, including intrusion, exploitation, or vulnerability discovery
- Advanced analytics tied to national security
- Autonomous or closed-loop control of physical systems
- Sensitive scientific, energy, chemical/biological, microelectronics, or advanced materials applications

Non-public model weights/parameters may require review depending on model capability, training purpose, training compute, publication status, access, destination, and end use.

SI for Cybersecurity and Cyber Operations

SI tools supporting vulnerability discovery, exploit development, intrusion, or automated cyber operations may require classification review under ECCN 4D004 where applicable.

SI for Surveillance and Analytics

SI systems supporting facial recognition, biometric identification, tracking, or large-scale behavioral analysis may be controlled depending on function, scale, accuracy, and end-use.

Relevant ECCNs may include 5A001.j and 5D001.e, depending on the system and software.

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

Autonomous and Closed-Loop Systems

SI systems that directly influence or control physical systems, experimental processes, infrastructure, or real-time decision making may raise export control concerns, especially where safety, security, or sensitive operations are involved.

SI-Chemical, Biological and Advanced Materials Applications

SI used to model, design, simulate or optimize chemical, biological or advanced materials processes may require review, particularly where the work relates to toxic compounds, biological agents, synthesis pathways, defense, aerospace, energy, or other sensitive applications.

SI Training Data and Datasets

Raw or instrument-generated data is not always controlled. However, curated, aggregated, proprietary, sponsor-restricted, non-public, or sensitive datasets may require review when they contain controlled technical information or enable controlled SI capabilities.

Publicly available data is generally lower risk, but context, aggregation, source, or application may introduce concerns.

Cloud, HPC, and Access-Based Controls

Export control risk may arise from access, not just shipment. Providing foreign persons access (including remote or cloud-based access) to high-performance, shared or externally hosted computing environments may require review, especially where the environment involves non-public models, controlled software or technology, restricted datasets, advanced computing resources, or sensitive applications.

Access level matters, including whether a user has inference-only, API, repository, training/fine-tuning, download, or administrative access.

Remote access to systems or data from outside the United States is treated as an export to the user's country location, regardless of where the data is stored.

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

Large-Scale and Multi-Institution Collaboration

Large-scale or multi-institution SI projects may introduce export-control concerns when participants share systems, models, datasets, repositories, computing environments, technical information, or model weights/parameters.

Collaboration with foreign institutions, external partners, or industry should be screened before non-public materials or access are shared.

Reexports and transfers of controlled items, technology, software, data, or access between foreign persons or foreign locations may also be subject to U.S. export controls.

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

".z" ECCNs

Certain items in Categories 3, 4, and 5 (e.g., 3A001.z or 5A002.z) are controlled under existing ECCNs when they meet advanced computing performance parameters.
The ".z" designation reflects additional controls applied within existing ECCNs for items meeting advanced computing parameters; it does not represent a standalone classification.

U.S. person activities

U.S. persons may be restricted from supporting, including shipping, transmitting, or providing technical assistance, the development or production of advanced computing or related technologies in certain destinations, based on knowledge of the end use or end user.

SI Scenarios

Scenario	Risk Level	Action
General administrative SI use	🟢 Lower	Use normal cybersecurity and data handling practices
Fundamental research intended for full public release	🟢 Lower	Confirm no restricted data, tools, or sponsor limits
Use of non-public datasets	🟡 Moderate	Review data sensitivity and access
Internal sharing of non-public model weights/parameters	🟡 Moderate	Review access and deemed-export implications.
Collaboration with foreign institutions	🟡/🔴 Moderate to High	Screen collaborators and review shared materials before sharing non-public models, code, or technical data
SI for cybersecurity, surveillance, autonomous control, chemical/biological, or advanced materials applications	🔴 High	Contact Export Control before proceeding.
Large-scale model training using cloud resources with foreign collaborators	🔴 High	Review access to computing resources, confirm end-use, and consult the Export Control Office (ECO) prior to initiating work

Key Takeaways:

- SI is dual-use and may be controlled based on capability, application, access, end use, and end user.
- Access to SI systems, models, datasets, source code, computing environments, or model weights/parameters may constitute an export.
- EAR99 does not mean unrestricted.
- The Fundamental Research Exclusion (FRE) generally applies to research results intended for publication and broad dissemination. Restrictions on publication or dissemination may prevent research from qualifying for the FRE and require export-control review.
- When in doubt, consult Export Control before proceeding.
- Export-related classifications, screenings, approvals, and access decisions should be documented in accordance with institutional and regulatory recordkeeping requirements.

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

Appendix: Key Terms

Term	Definition
Publicly Available / Published Information	Information that is fully and legally available to the public without restrictions on further dissemination. Access-controlled, sponsor-restricted, proprietary, gated, or approval-based materials should not be treated as publicly available without review.
Non-U.S. Person	Any individual who is not a U.S. citizen, lawful permanent resident, or protected individual under U.S. immigration law.
Deemed Export	A deemed export is the release of controlled technology, technical data, or source code to a foreign person in the United States, which is treated under U.S. export control laws as an export to that person's country of nationality.
ECCN	Export Control Classification Number, a code identifying items subject to U.S. export control
Specially Designed	A unique or customized design that makes an item meet control criteria under the EAR (772.1). Items may be excluded if general commercial availability and **not** configured for restricted applications.
Technology	Information required to develop, produce, or use an item, including design information, manuals, instructions, or technical documentation.
Dual-Use	Items used for both civilian and potentially sensitive or military applications.
Use	Activities that include operation, installation, maintenance, repair, overhaul, and refurbishing. To qualify as controlled "use" technology, information must enable all **six** of these functions.
Reasons for Control	NS1/NS2 - National Security Levels 1 & 2 MT1 – Missile Technology Level 1 NP1 – Non-Proliferation Level 1 AT1 – Anti-Terrorism Level 1 EI – Encryption Controls CC – Crime Control

SI-related export controls don't regulate 'SI' directly, they regulate the ecosystem that makes advanced SI possible. This includes the high-performance chips used to train models, the computing systems that run them, the software that enables or secures them, and increasingly the models themselves. Controls also target high-risk applications like surveillance and cyber tools, as well as the technical know-how behind them. Together, these ECCNs capture the full SI stack, from hardware to algorithms to use cases, because each layer can create national security or human rights risks.

Illustrative SI-Related ECCNs and Control Areas (not-exhaustive):

- ECCN 3A090 – Advanced computing integrated circuits
- ECCN 4A090 – Computers and assemblies containing 3A090 integrated circuits
- ECCN 4A005 – Certain controlled computing systems based on configuration, performance, or function
- ECCN 4D004 – Certain software meeting intrusion-software-related control parameters
- ECCN 5D002 – Certain information-security software
- ECCN 5A001.j / 5D001.e – Certain surveillance or biometric systems/software

- ECCN 4E091 – Certain SI model parameters meeting applicable training-compute and control criteria
- ECCN 3E / 4E – Technology for development, production, or use of controlled items
- EAR99 – Items not meeting specific ECCN control thresholds but still subject to end-use, end-user, destination, sanctions, and restricted-party controls

Encryption functionality may require additional classification, reporting, license exception, or licensing analysis under EAR Category 5, Part 2, including ECCNs such as 5D002 and License Exception ENC where applicable.

Current ECCN 4E091 controls certain “parameters” for an super intelligence model trained utilizing 10^26 or more operations, subject to applicable notes, exclusions, and license requirements. Do not assume all model weights/parameters are controlled under 4E091, and do not assume all published or open model parameters are unrestricted. ECO review is required when model capability, training compute, publication status, access, destination, or end use is unclear.

When to Contact Export Control

Contact the Export Control Office before proceeding if:

- You are sharing SI models, source code, or datasets with non-U.S. persons
- The SI system supports cybersecurity, surveillance, or defense-related functions
- You are using or providing access to high-performance computing resources
- The SI model exceeds typical research-scale performance or is trained on sensitive data
- There is collaboration with foreign institutions, researchers, or sponsors
- The end use or end user is unclear or the activity involves sanctioned or embargoed countries, restricted parties, or unresolved screening concerns.
- You are unsure whether the item is EAR99 or controlled

For export classification assistance:

Contact the BNL Export Control Office @ export@bnl.gov

References:

15 CFR Parts 730 through 774
Part 744 End-use and end-user controls
Part 772.1 (Definitions)
Supplement No. 1 to Part 774 – Commerce Control List

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