Brookhaven National Laboratory

FOCUS:

Super Intelligence (SI)

Export Control Guide for Determining the ECCN of Super Intelligence Technologies

Purpose

This document provides guidance for identifying the correct Export Control Classification Number (ECCN) for Super Intelligence (SI) technologies, systems, software, and associated technical data. It focuses on classification criteria and parameters under the U.S. Department of Commerce Export Administration Regulations (EAR), and where applicable, highlights when escalation is required.

How to use this Document: Use this guide for determining the applicable ECCN for SI technologies, software, systems, and related technical information. For broader export-control risks and regulatory considerations, refer to the *SI – Export Control Guidance and Risk Considerations*. 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.*

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

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 is determined to be subject to the International Traffic in Arms Regulations (ITAR), STOP — this guidance does not apply. Immediately consult the Export Control Office before any access, use, or transfer.*

What's Controlled? – The Big Picture

Super Intelligence technologies are considered dual-use. They support a wide range of civilian and research applications (e.g., healthcare, energy systems, climate modeling, and scientific discovery), but also have significant potential for military, intelligence, cybersecurity, and surveillance applications.

Because of this dual-use nature, export controls apply to:

- Hardware (e.g., specialized SI chips, accelerators, and high-performance computing systems)
- Software (e.g., SI/ML foundation models, training frameworks, and inference engines)
- Technology (e.g., algorithms, model architectures, training methods, datasets, and documentation)

SI items become export controlled when their performance, scale, capability, or intended application exceeds regulatory thresholds, or when they are "*specially designed*" for controlled or sensitive applications.

KEY SI Areas of Concern

SI Compute and Hardware

Advanced computing systems designed for training or running large-scale SI models may be controlled based on performance metrics such as processing speed, interconnect bandwidth, or aggregate compute capability. Certain high-performance integrated circuits and computing clusters fall under ECCNs such as 3A090 or related controls. Systems incorporating such chips may fall under ECCN 4A090, while other computing equipment may be classified under 4A005 depending on configuration and performance.

Note: Restrictions may also apply to providing foreign persons access to U.S. cloud-based High-Performance Computing (HPC) or Infrastructure as a Service (IaaS) for the purpose of training large SI models.

SI Models and Software

SI software, including machine learning models, may be controlled when designed for:

- Military, intelligence, or surveillance applications
- Cyber operations (e.g., intrusion, exploitation, or vulnerability discovery)
- Advanced analytics tied to national security

Controls may apply to both source code *and* object code. Certain advanced SI model weights may be subject to emerging regulatory controls (e.g., ECCN 4E091 or similar frameworks) and should be reviewed with Export Compliance.

SI for Cybersecurity and Cyber Operations

SI tools designed for penetration testing, exploit development, or automated cyber operations may fall under ECCN 4D004 if they meet intrusion software criteria.

SI-Enabled Data Analysis and Surveillance

Systems designed for facial recognition, biometric identification, or large-scale behavioral analysis may be controlled depending on accuracy, scale, and end-use, including under ECCNs such as 5A001.j and 5D001.e.

Autonomous Systems and Decision-Making

SI enabling autonomous navigation, targeting, or decision-making in drones, robotics, or vehicles may be subject to control, particularly if integrated into defense or surveillance systems.

SI Training Data and Datasets

While raw data is not always controlled, curated datasets, especially those tied to defense, intelligence, or sensitive infrastructure may be subject to restrictions when they enable controlled SI capabilities.

How to determine the correct ECCN

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

1. Confirm the item's purpose and design intent.

Is the SI system designed for general research, or for sensitive applications such as cybersecurity, surveillance, or defense?

2. Evaluate performance and capability

Does the system exceed thresholds for computing performance, model scale, or functional capability?

3. Identify if the item is specially designed

Was the SI system or model customized for a controlled application or user?

4. Match to applicable ECCN categories

Common categories include **Category 3**: Electronics (advanced computing hardware) **Category 4**: Computers (high-performance computing and software) **Category 5**: Telecommunications and Information Security (encryption, secure communications)

5. Determine applicable controls

Hardware: “A” ECCNs (e.g., 3A090, 4A090, 4A005) **Software**: “D” ECCNs (e.g., 4D004, 5D002) **Technology:** “E” ECCNs (e.g., 3E, 4E, 4E091)

6. Assess end use and end user controls

Consider Part 744 “catch-all” controls, including restrictions related to advanced computing, military end use/end users, and prohibited parties. Certain items may fall under “.z” ECCNs or require licensing based on end use even if not explicitly listed.

7. Uncertain?

Consult the Export Control Office before sharing SI models, datasets, or technical information.

Note: If an item is subject to the EAR but is not classified under a specific ECCN, it may be designated EAR99. However, EAR99 does not mean unrestricted. Export restrictions or licensing requirements may still apply based on the destination, end use, end user, applicable sanctions, or restricted-party controls. Contact the Export Control Office when classification or authorization requirements are unclear.

Contact the Export Control Office BEFORE proceeding if any of the following apply:

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 could involve restricted applications - You are unsure whether the item is EAR99 or controlled

Note on Deemed Exports

Providing foreign nationals (including employees, researchers, or collaborators in the United States) with access to controlled SI models, software, source code, or detailed technical information may constitute a “deemed export.” This includes access through shared repositories, cloud platforms, or interactive model interfaces where underlying capabilities or controlled technology can be learned or extracted. Such access may require prior export authorization even if no physical transfer occurs.

Key Terms:

Term	Definition
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 of general commercial availability and **not** configured for restricted applications.
Technology	Information required to develop, produce, or use an item (may include design, manuals, and instructions)
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

Key Takeaways:

- SI systems, software, or related technology may require export authorization depending on classification, destination, end use, and end user, including certain items designated EAR99.
- Consult the Export Control Office before sharing SI-related items internationally or with foreign nationals.
- Document how each ECCN determination was made.
- Reassess classifications as SI models, capabilities or applications evolve.

Illustrative SI-Related ECCNs (not-exhaustive):

ECCN 3A090 – Advanced computing integrated circuits
ECCN 4A090 – Computers and assemblies containing 3A090 chips
ECCN 4A005 – Other controlled computing systems based on configuration/performance
ECCN 4D004 – Intrusion software
ECCN 5D002 – Information security software
ECCN 5A001.j / 5D001.e – Surveillance and biometric systems/software
ECCN 4E091 – Certain advanced SI model weights (emerging controls)
ECCN 3E / 4E – Technology for development, production, or use
EAR99 – Items not meeting control thresholds

References and Contacts:

15 CFR Part 774 Categories 3, 4, 5
15 CFR 772.1 (Definitions)
Supplement No. 1 to Part 774

For export classification assistance, contact the BNL Export Control Office @ export@bnl.gov

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