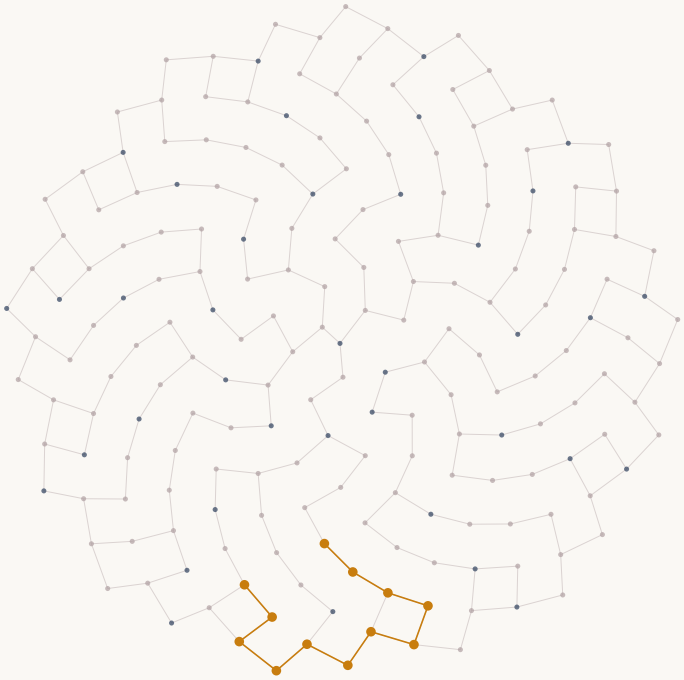
A SAYARI EXPORT CONTROLS BLOG . JUNE 2025 . SAYARI ANALYST TEAM



Screening Address-Only Entity List Entries

BIS uses addresses as entity identifiers on the Entity List when company names can't be verified.

Here's what that means for export compliance screening programs.

By Sayari Analyst Team . Published June 2025 . sayari.com

EXPORT CONTROLS

Screening Address-Only Entity List Entries

By Sayari Analyst Team · Published June 2025

BIS uses addresses as entity identifiers on the Entity List when company names can't be verified. Here's what that means for export compliance screening programs.

Export screening has assumed name-based matching: receive a customer name, check against lists, flag matches. That worked when all Entity List entries included verified names. But a growing portion identifies restricted locations with only an address-creating a blind spot that leaves companies vulnerable to shipping controlled goods while name-based systems return zero alerts.

BIS address-only entries are not theoretical. Companies have faced enforcement action for transactions involving these parties-with no way to detect them.

Why BIS Uses Address-Only Entries on the Entity List

The Entity List includes company names, addresses, and countries. This works for known entities with registered presence. But end-use intelligence often identifies locations rather than legal entities. A facility in Shanghai may divert equipment into weapons development, but the operator may have no registered name, changes names frequently, or operates covertly. Publishing an unverified name exposes BIS to liability. Publishing only the address solves this while preserving list integrity. This occurs in China, Russia, and countries with opaque registries where state-owned enterprises use shells. When BIS cannot link a location to a single verifiable entity name, the address becomes the control point. The message is clear: know who receives your goods at that location.

The legal effect is identical to a named entry: parties at that address are subject to license requirements, and beneficial owners controlled by sanctioned entities may be controlled

regardless of whether the company name appears on public lists. But screening address-only entries requires capabilities most export compliance programs lack. Name-based screening compares customer names against list entries. This fails when entries contain no name. A Shanghai buyer's registered name may find no hits because the address-only entry records coordinates, not company names. The consequence is undetected exposure. Semiconductor equipment shipped to an address-listed location via a shell company should trigger license requirements but instead passes screening. Name-and-country-code screening misses address-only entries entirely. A Beijing buyer's registered name receives no scrutiny; the actual delivery address-a known weapons network node-never enters the algorithm.

The Screening Challenge: Name-Based Systems vs. Address-Only Entries

The fundamental problem is that companies screen using customer names and company identities-information they collect during sales transactions. But address-only Entity List entries don't identify entities by name; they identify by location. When a customer requests equipment delivery to an address, that address is typically a production facility or warehouse location, not the legal entity's registered address. The customer's legal entity address may be on the other side of the country. This mismatch between the legal entity screened and the actual delivery location created the compliance gap that address-only entries now expose.

The fix requires address-based screening: geocoding customer delivery addresses, standardizing formats across registries, checking whether stated locations match Entity List addresses. When found, perform reverse lookup to identify entities at that location, then trace beneficial ownership to determine control by known Entity List parties. This requires corporate registry access across 250+ jurisdictions, address standardization and geocoding at scale, and network analysis to trace ownership relationships. OFAC's 50% Rule subjects entities 50%+ owned by sanctioned parties to sanctions, regardless of whether they appear on lists. BIS operates similarly: entities controlled by Entity List parties inherit license requirements even without direct listing. A Moscow facility uses an address flagged on the Entity List but operates under an innocuous subsidiary name. Name screening misses it. But if the subsidiary is 50%+ owned by a parent on the Entity List, the transaction requires a license anyway. Address screening catches location; network analysis catches ownership. Address-based screening combined with corporate family tracing surfaces parent-subsidiary relationships that name-based screening cannot detect.

Four Capabilities Required for Address-Based Screening

Screening address-only entries requires four integrated capabilities that most export compliance programs lack. First, corporate registry lookup by address. Query registry data to identify all entities at a customer's location-a location-based discovery process, not a name match. This requires access to corporate registry databases in China, Russia, and other high-risk jurisdictions, where companies may operate across multiple locations.

Second, standardized geocoding and address normalization. Addresses come in dozens of formats and languages. Russian Cyrillic, Chinese Pinyin, and English Roman characters may identify the same location but appear different without normalization. Street numbers may be represented as " 1 " in Chinese or "ul. 1" in Russian. Geocoding converts addresses to standardized coordinates; reverse geocoding converts coordinates back to standardized formats. At scale, this requires commercial geocoding infrastructure and address standardization rules specific to each jurisdiction.

Third, network analysis tracing connections between listed and unlisted entities. When an address matches an Entity List entry, identify beneficial owners, parents, directors, and related entities. If any are listed, the customer inherits compliance obligations. This requires ownership data and corporate hierarchies across jurisdictions. When a subsidiary at an address-flagged location is 60% owned by a parent company that doesn't appear on the Entity List but whose beneficial owner is sanctioned, that ownership relationship becomes the enforcement liability. Network analysis must trace these multi-hop ownership chains.

Fourth, integrate address data into onboarding and ongoing screening. Require complete customer addresses; run address screening as automatically as name screening. Failures should trigger the same alerts as direct matches. But "complete customer addresses" is more complex than it sounds-customers may provide legal entity addresses, billing addresses, and delivery addresses. Each may be different. A production facility address where equipment will be delivered is distinct from the legal entity's corporate headquarters. Screening must account for this distinction.

Moving Forward: The Business Case and Compliance Imperative

The infrastructure exists-databases covering 250+ jurisdictions, address matching across 400+ million entities, beneficial ownership network analysis-but requires deliberate investment. Most enforcement actions involved named parties, so teams haven't prioritized this. As BIS adds address-only entries, that stance becomes untenable. The shift toward address-only entries reflects changed threat landscapes and intelligence capabilities. It signals covert nodes that BIS cannot name but can locate. Exporters relying solely on name screening ignore a growing Entity List portion.

Address-based screening is no longer optional for companies with China, Russia, or similar supply chains where shells and covert nodes operate. The technical effort is real, but so is the gap without it. Sayari's Global Trade Compliance platform integrates address-based entity screening with network analysis across 400+ million corporate entities and 250+ jurisdictions, enabling compliance teams to catch restricted locations and beneficial owners simultaneously. The platform's entity resolution and corporate family tracing capabilities surface the ownership chains that name-based screening alone cannot detect.

For export control officers looking to close the address-only Entity List gap, the first step is auditing whether your current screening program has address-based matching capabilities at all. If not, that gap represents real enforcement risk. Request a demo to see how address and network-based screening can strengthen your export control program.

Please visit sayari.com to learn more.

This blog is for informational purposes and isn't intended to be legal advice.