WHITEPAPER

ITAR Visitor Screening & Access Control

Meeting 22 CFR 120-130 Foreign National Requirements

How defense contractors can implement systematic visitor screening workflows to satisfy ITAR foreign national access requirements — and avoid penalties up to $1,000,000 per violation.

ITAR (22 CFR) | EAR (15 CFR) | DDTC | OFAC SDN

$1M	20yr	5yr	60d
Per Violation	Criminal Penalty	Record Retention	Implementation

SecurePoint USA

SAM.gov Registered · Active CAGE Code · Built for Defense Contractors

securepointusa.com

2026

Originally published: 2026-04-01 Last reviewed: 2026-05-09

01 Executive Summary

The International Traffic in Arms Regulations (ITAR), codified in 22 CFR Parts 120-130, impose controls on who can access defense articles, technical data, and defense services. Under the "deemed export" rule (22 CFR § 120.54), releasing controlled technical data to a foreign person — including on U.S. soil — is generally treated as an export to that person's country of nationality.

A visitor entering a facility where ITAR-controlled data exists represents a potential export-control event. Penalty maximums are set and periodically adjusted by DDTC; civil and criminal exposure can be significant, and DDTC generally applies strict liability — accidental exposure can carry the same consequences as a deliberate violation. Confirm current penalty figures with your export-control counsel before relying on any specific dollar amount.

A foreign national who views a controlled schematic, walks through a production area where USML-classified items are present, or hears a technical discussion about a defense article may trigger a deemed export — regardless of intent.

This whitepaper walks through five common failure points in ITAR visitor management, outlines a defensible screening workflow, summarizes recent DDTC enforcement actions, and provides a 60-day implementation roadmap. It is not legal advice; consult qualified export-control counsel before relying on anything here.

02 The ITAR Framework for Physical Access

US Person vs. Foreign Person (22 CFR § 120.62 / § 120.16)

ITAR defines a "US Person" as a US citizen, lawful permanent resident, protected individual under 8 U.S.C. § 1324b(a)(3), or any entity incorporated in the US. Everyone else is a "foreign person." This determination is the threshold question for every visitor — and it must be made before access is granted.

Dual nationals present additional complexity. A visitor who holds both US and foreign citizenship is generally treated as a US Person, but specific country combinations may trigger additional screening requirements under sanctions programs.

Deemed Exports (22 CFR § 120.54)

The release of controlled technical data to a foreign person in the United States is "deemed" to be an export to the country of the foreign person's nationality. This includes visual access (seeing a controlled document), verbal disclosure (discussing controlled specifications), and physical access (entering a space where controlled articles are present).

A foreign visitor walking through a manufacturing floor where USML items are being assembled has received a deemed export — even if they weren't shown anything specific. The physical presence in the controlled area is sufficient.

Technology Control Plans (TCP)

A Technology Control Plan defines how a facility physically and procedurally separates controlled from uncontrolled areas. TCPs typically specify which zones require ITAR clearance, which require escort, and which are accessible to all visitors. A visitor management system that enforces the TCP — rather than merely documenting it — provides stronger evidence than process documentation alone.

Record-Keeping Requirements (22 CFR § 122.5)

ITAR-registered manufacturers and exporters must maintain records of all exports and deemed exports for a minimum of five years. For visitor management, this means retaining visitor identity, nationality, screening results, zone access logs, escort assignments, and any technical data access documentation for every foreign visitor.

03 The 5 Critical ITAR Failure Points

DDTC enforcement actions consistently reveal the same five gaps in how defense contractors manage visitor access. Each one independently creates deemed export exposure.

- **No Citizenship Verification at Registration** 22 CFR § 120.62
  Most visitor management systems collect a name and a company. They do not ask for citizenship, dual nationality status, or country of origin. Without this data, you cannot determine whether a visitor is a US Person under ITAR.
- **No Pre-Arrival Screening** 22 CFR § 127.1
  Foreign nationals must be screened against the OFAC SDN list, BIS Entity List, BIS Denied Persons List, and DDTC Debarred Parties List before they arrive on site. Screening after arrival means a restricted person may have already accessed controlled data.
- **No Zone-Based Access Enforcement** 22 CFR § 125.4
  ITAR-controlled areas must be physically and logically separated from uncontrolled areas. A visitor badge that grants access to the entire facility creates uncontrolled deemed export exposure for every foreign visitor.
- **No Mandatory Escort Workflow** 22 CFR § 126.18
  Foreign nationals in ITAR-controlled areas must be escorted at all times. An optional escort field on a check-in form does not constitute escort enforcement.
- **No Defensible Audit Trail** 22 CFR § 122.5
  DDTC expects documentation of who accessed what, when, and under what authorization. Visitor logs that can be edited or deleted do not constitute defensible compliance evidence.

Each failure point can independently create exposure. A foreign visitor who arrives unscreened, enters a controlled zone without escort, and is not captured in an audit trail can represent multiple potential ITAR exposures at once — and the absence of records makes after-the-fact disclosure harder. Penalty figures are set by DDTC and change; consult counsel for current numbers.

04 Building a Compliant Screening Workflow

A defensible ITAR visitor management workflow has five distinct phases — each generating compliance evidence that auditors and DDTC investigators expect to see.

Phase 1: Pre-Registration

- Citizenship and dual nationality collected at invitation
- Country of origin evaluated against embargoed nations
- Company affiliation screened against BIS Entity List
- Purpose of visit documented with technical data access scope
- Government-issued photo ID uploaded for verification

Phase 2: Pre-Arrival Screening

- Automated screening against OFAC SDN, BIS Entity List, BIS Denied Persons, DDTC Debarred Parties
- Fuzzy matching catches name variations and transliterations
- Foreign person status determination under 22 CFR § 120.62
- License exception eligibility evaluation (NLR, STA, TSU, TMP)
- Compliance officer notification for matches

Phase 3: Arrival & Check-In

- Re-screening catches list updates between pre-registration and arrival
- Government ID verified against pre-registration data
- Zone access determined by visitor export classification
- Mandatory escort assignment and confirmation
- Badge issued reflecting approved access posture

Phase 4: During Visit

- Escort acknowledgment tracked with timestamp
- Zone transition logging for visitors in controlled areas
- Automatic alerts for overstay or restricted area access attempts
- NDA capture for visitors accessing controlled technical data

Phase 5: Post-Visit

- Automated after-visit report with escort compliance data
- Technical data access documentation linked to classifications
- Badge return confirmation and deactivation logged
- Complete evidence pack exportable in CSV, PDF, JSON
- Immutable audit trail retained for 5-year ITAR requirement

05 DDTC Enforcement: Real-World Consequences

Recent DDTC consent agreements demonstrate that export control violations — including inadequate access controls for foreign persons — result in significant financial penalties, mandatory compliance programs, and reputational damage.

- **FLIR Systems — $30 million (2023)**
  Unauthorized exports of ITAR-controlled thermal imaging technology. Violations included inadequate screening of foreign national employees and visitors with access to controlled data.
- **Honeywell International — $13 million (2023)**
  Unauthorized exports of technical drawings related to aircraft engines, guidance systems, and other defense articles. Failures included inadequate access controls for foreign persons.
- **L3Harris Technologies — $13 million (2023)**
  ITAR violations involving night vision and electro-optical technology. Included failures in TCP implementation and monitoring of foreign national access.

- **Curtiss-Wright — $2.85 million (2023)**
  Unauthorized exports of technical data related to defense electronics. Violations stemmed from inadequate internal controls over foreign person access.

Voluntary self-disclosure (VSD) under 22 CFR § 127.12 is treated as a mitigating factor but does not eliminate penalties. The best protection is prevention — not disclosure after the fact.

06 Technology Control Plan Integration

Your Technology Control Plan defines the rules. Your visitor management system enforces them. The two must be tightly integrated.

Zone-Based Access Classification

Map your facility into export control zones: ITAR-controlled, EAR-controlled, restricted, and unclassified. Each zone carries its own access requirements, escort rules, and badge-level permissions. Visitors are assigned to zones based on their export classification — not based on who they're visiting.

Export Classification Management

Visitors, their companies, and specific visits can each carry export classifications — USML categories (I-XXI), ECCN codes, or program-specific tags. Classifications determine zone eligibility and trigger appropriate screening workflows. Classifications can expire, requiring re-evaluation for repeat visitors.

License Exception Tracking

Not all foreign person access requires a full export license. License exceptions (NLR, STA, TSU, TMP) may apply. Your system must track which exception applies, document the basis, and retain this as part of the 5-year record-keeping requirement.

07 SecurePoint USA ITAR Capabilities

Foreign Person Status Determination

Citizenship and nationality are captured at pre-registration as required data. The system evaluates US Person status under 22 CFR § 120.62, flags dual nationals, and screens country of origin against embargoed nations. If status cannot be confirmed, badge issuance is blocked until an export control officer reviews and approves.

Multi-List Sanctions Screening

Every visitor is screened against OFAC SDN, BIS Entity List, BIS Denied Persons, DDTC Debarred Parties, EU FSF, and UK Sanctions lists. Screening occurs at pre-registration and again at check-in. Fuzzy matching with configurable thresholds catches name variations. Matches trigger automatic hold until compliance officer adjudication.

Zone-Based Access & TCP Enforcement

Site export zones map directly to your TCP. Each zone defines access requirements. Visitor badges reflect the approved access posture. Zone transitions are logged. Foreign nationals are automatically routed to approved zones only.

Mandatory Escort Enforcement

Foreign nationals in controlled zones require confirmed escorts. Badge issuance is blocked until an escort from the

authorized roster accepts. Notification, acknowledgment, and escalation are automated. No foreign visitor can enter a controlled area without a confirmed, active escort.

Immutable Audit Trail

Every screening result, access decision, escort assignment, zone transition, and badge event is recorded in an append-only, cryptographically hashed audit log. Records cannot be edited, deleted, or backdated by anyone. Data retained for the full ITAR 5-year requirement. Exportable in CSV, PDF, and JSON.

08 60-Day Implementation Roadmap

Week 1-2: Discovery & TCP Mapping

- Audit current processes and document gaps against 22 CFR
- Map facility zones to export control classifications
- Identify USML categories and ECCN codes per facility
- Define escort policies per zone and visitor type

Week 3-4: Platform Configuration

- Configure site zones matching your TCP
- Set up multi-list screening rules and thresholds
- Define badge templates for each access posture
- Configure escort notification and escalation chains

Week 5-6: Testing & Training

- Run screening tests across nationality/zone combinations
- Train front desk staff on kiosk operations
- Train export control officers on adjudication dashboard
- Validate audit trail completeness for every event type

Week 7-8: Go-Live & Validation

- Deploy with parallel operation alongside existing processes
- Monitor screening results and adjudication workflows
- Generate first compliance evidence export
- Schedule 30-day post-launch compliance review

SRC Sources & Notes

The references below are the primary sources used in this paper. They are listed for traceability and verification — they are not endorsements, and SecurePoint USA does not represent any source as exhaustive. Confirm current text and guidance with the source itself before relying on any citation.

[1] International Traffic in Arms Regulations — 22 CFR Parts 120-130

https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M

Primary source for definitions of "US person," "foreign person," "deemed export," and recordkeeping obligations.

[2] Export Administration Regulations — 15 CFR Parts 730-774

https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C

EAR framework, ECCN structure, and license exceptions referenced.

[3] DDTC Penalties and Oversight Information

https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=384b968adb3cd30044f9ff621f961941

Source for the consent agreements summarized in the enforcement section. Penalty figures and dates may be revised; reconfirm against the official DDTC notice before quoting.

[4] BIS Consolidated Screening List

https://www.trade.gov/consolidated-screening-list

Authoritative starting point for the multi-list screening discussion (SDN, Entity List, Denied Persons, DDTC Debarred, etc.).

Originally published: 2026-04-01 Last reviewed: 2026-05-09

From Paper Compliance to Operational Controls

A foreign visitor who enters a controlled space without screening, escort, or a recorded audit trail can create real export-control exposure. A systematic intake-to-checkout workflow turns each visit into evidence rather than risk.

SecurePoint USA provides foreign-person determination support, multi-list sanctions screening, TCP-aligned zone enforcement, escort workflows, and immutable audit trails. A typical greenfield deployment lands in roughly 60 days; complex environments take longer.

Schedule a Compliance Review

securepointusa.com/request-demo

SAM.gov Registered · Active CAGE Code · Built for Defense Contractors

 Last reviewed: 2026-05-09

This whitepaper is provided for general informational purposes only and does not constitute legal, regulatory, export-control, or compliance advice.

It is not a substitute for review by qualified counsel, a C3PAO, your Facility Security Officer (FSO), an export-control or empowered official, sanctions counsel, or other advisor familiar with your specific contracts, facilities, and obligations.

Regulatory citations, enforcement examples, and statistics reflect publicly available information believed to be accurate as of the "Last reviewed" date on the cover page. Regulations and enforcement priorities change; consult primary sources before acting on anything in this document.

Statements about SecurePoint USA capabilities describe current product behavior, not a contractual commitment. Capability fit for any specific environment must be confirmed during scoping.