SecurePoint USA

Whitepaper



ITAR visitor screening and access control

Controlling foreign-person access to technical data under the ITAR deemed-export rule

ITAR · EAR · NISPOM

A guide for export-control officers, empowered officials and facility security officers who host visitors where ITAR technical data is present. It explains when a visit becomes an export under the ITAR and the EAR, how U.S.-person status is defined and recorded, what a Technology Control Plan and the NISPOM say about escorts, which records to keep, and where penalties and disclosure duties begin. Statements about SecurePoint are kept apart from the rules.

Written for

Export-control officers, empowered officials, facility security officers

Last reviewed

November 7, 2026

First published

March 16, 2026

Read online

securepointusa.com/resources/whitepapers/itar-visitor-screening

Informational only. Not legal, regulatory, export-control, or compliance advice. Not a substitute for review by qualified counsel or the compliance professionals who know your obligations.

Contents

1.	Executive summary	3
2.	When a visit becomes an export	4
3.	U.S. persons, foreign persons and dual nationals	5
4.	Technology Control Plans and escorts	6
5.	Screening visitors against restricted-party lists	7
6.	How SecurePoint handles a visit at an ITAR site	8
7.	Records and retention	10
8.	Penalties, disclosure and DDTC enforcement	11
9.	An implementation plan	12
	Sources and revision history	14
	About SecurePoint USA	17

Key takeaways

- The ITAR has no visitor rule. It controls releases of technical data to foreign persons, and a visit is one way a release can happen (22 CFR 120.50 and 120.56).
- Under the ITAR a release counts as an export to every country of the person’s citizenship, past or present, or permanent residency. The EAR counts only the most recent.
- Escort rules come from your Technology Control Plan, license provisos and, for cleared contractors under FOCI mitigation, the NISPOM (32 CFR 117.11(h)). The ITAR sets none.
- Knowing of an export to a § 126.1 country, which can include a release to one of its nationals, triggers an immediate notice to DDTC (22 CFR 126.1(e)(2)).
- A visitor system can hold a visit, require an escort and keep the record. It does not decide U.S.-person status or license need, and it does not make an organization compliant.

Last reviewed November 7, 2026 against the sources listed at the end of this paper and against SecurePoint's product as it stood that day.

1. Executive summary

The International Traffic in Arms Regulations (ITAR, 22 CFR parts 120 to 130) control the export of defense articles, technical data and defense services. Releasing technical data to a foreign person in the United States is an export (22 CFR 120.50(a)(2)), and a visit is one way a release can happen: a visitor examines a defense article closely enough to learn its technical data, reads a drawing, or hears a technical discussion (22 CFR 120.56(a)).

The ITAR has no visitor rule. It does not say who may enter a building or who needs an escort. Those controls come from an organization's Technology Control Plan (TCP), from the provisos on its licenses and agreements, and, for some cleared contractors, from the National Industrial Security Program Operating Manual (NISPOM). A visitor program is where those controls meet a person at the door, and where the record of the visit starts.

This paper covers when a visit becomes an export, how U.S.-person status is defined and recorded, what a TCP says about visitors, screening visitors against restricted-party lists, the records to keep, and where penalties and disclosure duties begin. Statements about SecurePoint appear in marked boxes and in section 6, apart from the rules.

What SecurePoint does and does not do

SecurePoint is visitor management and restricted-party screening software. At a site set to its ITAR Controlled or DCSA High Security profile, it screens each visitor, takes a U.S.-person attestation or foreign-national acknowledgment at every check-in, holds visits that need a compliance decision, keeps a visitor who needs an escort from being admitted or badged until one is named, and records each step in an append-only, hash-chained audit log that application users cannot edit or delete, with a verifier that checks the chain.

- It does not decide U.S.-person status, export classification, or whether a release needs a license or exemption. Your export-control officer or empowered official decides those.
- It does not track where a visitor goes inside a facility, connect to door hardware, or set up access zones. Escorts and physical access controls enforce the boundaries between areas.
- It records one country of citizenship per visit. Collect any other citizenship and permanent residency through your own visit request.
- It does not file anything with DDTC, BIS or OFAC, and it does not make an organization ITAR compliant.

2. When a visit becomes an export

Under the ITAR, an export includes releasing or otherwise transferring technical data to a foreign person in the United States, which the rule calls a deemed export (22 CFR 120.50(a)(2)). Section 120.56 says how a release happens:

> *Technical data is released through: (1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; (2) Oral or written exchanges with foreign persons of technical data in the United States or abroad; (3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or (4) The use of access information to cause technical data outside of the United States to be in unencrypted form.*
>
> 22 CFR 120.56(a)

In a visit, the first two are the usual routes: a visitor examines hardware closely enough to learn how it is designed or made, reads a drawing on a wall or a screen, or hears a technical discussion. Presence in an area is not the test on its own. What the route exposes is, and judging that belongs to your export-control officer.

A release is deemed an export to every country where the foreign person holds or has held citizenship or holds permanent residency (22 CFR 120.50(b)), not only the country of the passport they show. A release to a national of a country listed in 22 CFR 126.1 is therefore an export to a country for which the policy of the United States is to deny licenses and other approvals (22 CFR 126.1(a)).

The EAR works differently

Dual-use items, and military items moved off the U.S. Munitions List, fall under the Export Administration Regulations (EAR, 15 CFR parts 730 to 774), which control technology and source code rather than technical data. Releasing them to a foreign person in the United States is also a deemed export (15 CFR 734.13(a)(2)), and a release happens through visual or other inspection or through oral or written exchanges (15 CFR 734.15(a)). The country the export counts toward is different, and so is the record period.

Table 1. How the ITAR and the EAR treat a release during a visit

Question	ITAR (22 CFR)	EAR (15 CFR)
What is controlled	Technical data for defense articles on the U.S. Munitions List	Technology and source code for items subject to the EAR
A release in the United States	An export to the foreign person (120.50(a)(2))	A deemed export to the foreign person (734.13(a)(2))
Which countries count	Every country of citizenship, past or present, and of current permanent residency (120.50(b))	The most recent country of citizenship or permanent residency (734.13(b))

Question	ITAR (22 CFR)	EAR (15 CFR)
How a release happens	Visual inspection, oral or written exchanges, or access information (120.56(a))	Visual inspection, or oral or written exchanges (734.15(a))
How long records are kept	Five years from the expiry of the license or other approval, or from the date of the transaction (122.5(a))	Five years from the latest of the export, a known reexport or transfer, or the end of the transaction (762.6(a))

> **Classification decides which rule applies**
>
> Whether a technology falls under the ITAR or the EAR depends on its classification, which your export-control officer decides and which changes when the U.S. Munitions List or the Commerce Control List changes. Record which rule each controlled area falls under, because the countries that count differ.

3. U.S. persons, foreign persons and dual nationals

For an individual, a U.S. person under the ITAR is a lawful permanent resident or a protected individual as defined in 8 U.S.C. 1324b(a)(3): U.S. citizens and nationals, and certain others, such as people admitted as refugees or granted asylum (22 CFR 120.62). A foreign person is any natural person who is neither (22 CFR 120.63). Citizenship alone does not settle every case: a permanent resident or a refugee with no U.S. citizenship is a U.S. person.

Under the ITAR, a U.S. citizen is a U.S. person whatever other citizenship they hold. For a foreign person, the ITAR counts every country of citizenship or permanent residency, and the EAR only the most recent, so ask visitors before the visit for every citizenship, past and present, and any permanent residency.

Deciding a visitor’s status, and whether a release to them needs a license or an exemption, is the export-control officer’s job before the visit. Apply your facility policy without treating every ordinary visit as an export.

How SecurePoint records U.S.-person status

At a site set to the ITAR Controlled or DCSA High Security profile, every check-in takes a U.S.-person attestation or, from a visitor who gives another citizenship, a foreign-national acknowledgment, before a badge is issued. An answer from an earlier visit does not count. These sites check visitors in through the kiosk or the front desk's guided check-in, which ask for it.

Three answers hold the visit for compliance review: a country listed in § 126.1, checked against SecurePoint's copy of the list, which includes China, Russia, Iran, North Korea, Cuba, Venezuela, Belarus and Burma; a country that cannot be resolved; and a U.S.-person attestation given with a non-U.S. citizenship, because check-in cannot tell a permanent resident or a refugee from a mistaken answer. Confirm the current § 126.1 rule with your export-control officer.

SecurePoint records one country per visit, so record any other citizenship or residency in your own review.

4. Technology Control Plans and escorts

The ITAR sets no escort rule. Escort requirements come from your Technology Control Plan (TCP), from the provisos on your licenses and agreements, and, for some cleared contractors, from the NISPOM, which requires a TCP of those under a foreign ownership, control or influence (FOCI) mitigation or negation agreement and of others when the cognizant security agency (CSA) decides one is appropriate:

> *A TCP approved by the CSA will be developed and implemented by those entities cleared under a VT, PA, SSA and SCA and when otherwise deemed appropriate by the CSA. The TCP will prescribe all security measures determined necessary to reasonably prevent the possibility of access by non-U.S. citizen employees and visitors to information for which they are not authorized.*
>
> 32 CFR 117.11(h)(1)

VT, PA, SSA and SCA are a voting trust, a proxy agreement, a special security agreement and a security control agreement, the FOCI mitigation and negation agreements the paragraph names. The same paragraph says a TCP includes unique badging, escorts, segregated work areas and security indoctrination, as appropriate. The NISPOM speaks of non-U.S. citizens, a wider group than the ITAR's foreign persons because it includes permanent residents, so a TCP that serves both should say which test each control uses.

Outside those cases a TCP is a document an organization writes for its own program. Whatever its source, it describes the physical and procedural safeguards for controlled areas and data: which areas hold technical data, who may enter each, when a visitor needs an escort, and how staff keep technical data out of sight along an approved route.

What a visitor system can and cannot enforce

A visitor system can refuse to admit or badge a visitor until the conditions your TCP sets at the door are met, and record that they were. It cannot see what a visitor sees after the door. Staff, escorts and physical access controls keep a visitor on the approved route, and a badge or a cleared screening does not authorize an export.

> **Escort before admission**
>
> At ITAR Controlled sites a visitor who gives another citizenship, or whose status is unresolved, needs an escort; at DCSA High Security sites every visitor does, as does any visit classified as escorted with no unaccompanied ITAR access. A front-desk check-in stops until an escort is assigned, and no badge prints before then. No one can override a missing escort: the badge, the front desk's Admit step and SecurePoint's support tools all refuse until an escort is named.
>
> At a kiosk the visit waits for the front desk to assign an escort or, where the site's kiosk runs autonomous check-in, for the host to verify the visit and confirm the visitor's nationality on their ID, that they will escort the visitor at all times, and that they will not share export-controlled technical data without authorization. A visit held for a possible sanctions match keeps its escort requirement when the hold is cleared.
>
> Escort assignment, the host's escort confirmation and the end of the escort at check-out are recorded with timestamps. A U.S.-person attestation that no staff member or host verified also prints ESCORT: REQUIRED on the badge (section 6).

5. Screening visitors against restricted-party lists

No ITAR provision requires screening visitors, but several rules make it prudent. Without DDTC's written authorization, no one who knows a person is ineligible, a group that includes debarred persons, may take part in a transaction subject to the ITAR from which that person may benefit (22 CFR 127.1(d) and 120.16(c)). OFAC's sanctions bar U.S. persons from dealing with blocked persons, and the EAR restricts exports and releases of technology to parties on the Entity List and the Denied Persons List.

Screen every visitor, U.S. persons included: the lists name U.S. citizens and companies as well as foreign ones. Screen before arrival where you can, again at check-in, and on a schedule for visitors who return. A name match only nominates a candidate; the dates of birth, nationality and other identifiers on the list entry decide it, and a person should make that call.

What SecurePoint screens

By default, every visitor is screened against OFAC SDN and SSI, the BIS Entity List and Denied Persons List, and the UK, EU and UN sanctions lists, among other U.S. and international sources. The DDTC debarred list is carried in the platform but off until enabled: an administrator turns it on in the organization's screening settings and chooses whether a match holds the visit.

A visitor is screened at pre-registration. At check-in, the kiosk or the front desk's guided check-in screens again unless an approved screening is still inside the re-screening interval your organization sets and the name or ID given matches it.

Matches are scored against a configurable threshold, common names need a stronger match before they are flagged, and a person reviews every possible match. A possible match holds the visit and alerts your compliance managers, and no badge prints until a reviewer decides. The visitor's company is compared with listed entities as well; a company match holds the visit for review and does not block on its own.

Screening is not a national-origin rule

Export controls restrict releases of technology according to a person's status, not visits according to national origin. Where a visit is part of hiring, such as an interview, anti-discrimination law also applies: 8 U.S.C. 1324b and Title VII of the Civil Rights Act bar discrimination by national origin, and 8 U.S.C. 1324b bars discrimination by citizenship status against protected individuals unless a law, regulation, executive order or government contract requires it. Apply the same screening to every visitor, and tie escorts and holds to an export-control reason.

How SecurePoint applies citizenship

SecurePoint screens every visitor's name against the same lists, whatever their citizenship. Citizenship changes the outcome where a rule points to it: a visitor who gives a country under comprehensive U.S. sanctions, such as Cuba, Iran or North Korea, is held for sanctions review, and at an ITAR Controlled or DCSA High Security site a visitor not confirmed as a U.S. person is escorted rather than refused, unless one of the holds in section 3 applies.

6. How SecurePoint handles a visit at an ITAR site

What this section covers

This section describes SecurePoint at a site set to its ITAR Controlled or DCSA High Security profile, as it stood on the review date. If SecurePoint cannot read a site's profile, it refuses or holds the check-in rather than treating the site as unrestricted.

Table 2. What SecurePoint enforces and records at these sites, and what stays with your organization

Control	SecurePoint enforces	SecurePoint records	Your organization decides
Host	No check-in without a named host, chosen from the directory or typed in	The host on the visit	Which hosts may receive controlled visits
Identity	An ID captured at check-in; one uploaded at pre-registration does not count. A name or document number that differs from the pre-registration holds the visit for review.	The ID image and the comparison	What identity proof your TCP requires
U.S.-person status	An attestation or foreign-national acknowledgment at every check-in, and the compliance holds in section 3	The answer, the country given and any reviewer's decision	Status under 22 CFR 120.62 and 120.63, and any other citizenship
Screening	Screening at pre-registration and again at check-in; no badge while a possible match is under review	The result, the reviewer, the decision and its reason	Each possible match, and whether to turn on the DDTC list
NDA	A signed NDA before the visitor is admitted	The signed NDA and the version the visitor saw	The NDA's terms
Escort	An escort named before Admit or a badge for anyone who needs one, with no override	Escort assignment, the host's escort confirmation and the end of the escort, with timestamps	Escorting the visitor along the approved route
Areas	Nothing inside the facility: SecurePoint does not track movement or connect to door hardware	No movement inside the facility	The approved route and the physical controls that enforce it
After the visit	An after-visit report for every foreign national's visit, which cannot be switched off	The host's answers: whether controlled technology was shared, a description, and the ECCN if known; a yes sends an alert	Assessing any release and whether to disclose it
Audit trail	Application users cannot edit or delete entries	Each step in an append-only, hash-chained audit log with a verifier that checks the chain, kept for ten years	Your own records under 22 CFR 122.5

Table 3. What SecurePoint's ITAR badge template prints at these sites

Line	What it prints
Banner	ITAR RESTRICTED AREA, or DCSA HIGH SECURITY

Line	What it prints
Screening	SCREENED and the check-in date once screening has cleared, otherwise SCREENING: REVIEW
Escort	ESCORT: REQUIRED, unless the visitor is a confirmed U.S. person and no other escort rule applies
Status	US PERSON for a confirmed U.S. person, ESCORTED FOREIGN NATIONAL for a foreign national, and VERIFY ACCESS otherwise
Zone	ZONE: ESCORT ONLY, unless the visitor is a confirmed U.S. person; then ZONE: ITAR AREA or ZONE: HIGH SECURITY
Host	HOST: and the host's name

What a confirmed U.S. person means on the badge

A U.S.-person status counts as confirmed when staff ran the check-in, or a host verified the visit while signed in or with the one-time code from their arrival notice. A self-attestation at an unattended kiosk is not confirmed, so the badge prints escort only. Check that each controlled site uses this template or one with the same lines.

Badges do not print the areas your export-control officer approved for a visit, and SecurePoint has no zone setup.

7. Records and retention

Every person required to register with DDTC must keep records of the manufacture, acquisition and disposition of defense articles and technical data, of defense services and brokering, and of related political contributions, fees and commissions, including the documentation for exports made under licenses or exemptions (22 CFR 122.5(a)). A record may not be altered without recording the change, who made it and when.

> *All records subject to this section must be maintained for a period of five years from the expiration of the license or other approval, to include exports using an exemption (see § 123.26 of this subchapter); or, from the date of the transaction (e.g., expired licenses or other approvals relevant to the export transaction using an exemption).*
>
> 22 CFR 122.5(a)

This is not a rule to keep every foreign visitor's ID image or movement log. Have counsel decide which visit records support a covered activity and when their five years start. Under the EAR, records run five years from the latest of the export, a known reexport or transfer, or the end of the transaction (15 CFR 762.6), and OFAC requires ten years for records of transactions subject to its regulations (31 CFR 501.601).

What SecurePoint keeps

Screening completions, review decisions, escort assignments and badge prints are written to an append-only, hash-chained audit log that application users cannot edit or delete, with a verifier that checks the chain. Audit logs are kept for ten years.

Evidence and report exports cover screening activity, review decisions and the audit trail, with a SHA-256 checksum recorded for each export.

8. Penalties, disclosure and DDTC enforcement

Civil penalties under the Arms Export Control Act do not require intent. The maximum for each violation is the greater of $1,271,078 or twice the value of the transaction (22 CFR 127.10(a)(1)(i)), the figure set in January 2025; OMB Memorandum M-26-11 cancelled the 2026 inflation adjustment. Willful violations are crimes, with a fine of up to $1,000,000, up to 20 years in prison, or both, for each violation (22 U.S.C. 2778(c)).

Disclosure

The State Department strongly encourages voluntary disclosure of a possible violation to DDTC and may consider it a mitigating factor (22 CFR 127.12(a)); failing to report one will be an adverse factor. A disclosure starts with an initial notification immediately after a violation is discovered, and if that notification is incomplete, a full disclosure must follow within 60 calendar days (127.12(c)(1)). A disclosed violation can still be penalized (127.12(b)(3)).

One notice is not voluntary. Anyone who knows or has reason to know of a proposed or actual export of defense articles, defense services or technical data to a country listed in § 126.1, or to a person acting on its behalf, must inform DDTC immediately (22 CFR 126.1(e)(2)). Because a release is an export to every country where the recipient holds or has held citizenship or holds permanent residency, a release during a visit by a national of a § 126.1 country can bring this duty into play. Counsel should decide.

DDTC consent agreements

DDTC publishes its consent agreements. The six below involve technical data reaching foreign persons or foreign destinations, and the figures are the civil penalties the State Department announced.

Table 4. DDTC consent agreements involving unauthorized exports of technical data

Case	Civil penalty	What the State Department described
GE Aerospace (April 2026)	$36 million, $18 million suspended for remedial compliance	116 alleged violations, all voluntarily disclosed, including unauthorized exports of technical data to China. An external Special Compliance Officer and at least one external audit.

Case	Civil penalty	What the State Department described
BAE Systems, Inc. (August 2026)	$36 million, $18 million suspended for remedial compliance	104 alleged violations, all but one voluntarily disclosed, including unauthorized exports of technical data. An external Special Compliance Officer and at least one external audit.
The Boeing Company (February 2024)	$51 million, $24 million suspended for remedial compliance	199 alleged violations, all voluntarily disclosed, including unauthorized exports and retransfers of technical data to foreign-person employees and contractors, and unauthorized exports of technical data to China.
FLIR Systems (April 2018)	$30 million, $15 million suspended	Alleged unauthorized exports of technical data and defense services, including to dual-national employees from Iran, Iraq, Lebanon and Cuba who could reach technical data in company systems. DDTC said the company did not collect the citizenship information it needed to determine licensing requirements.
Honeywell International (April 2021)	$13 million, $5 million suspended	34 alleged violations, voluntarily disclosed, involving engineering drawings with technical data for parts of the F-35, F-22 and B-1B aircraft and the CTS800 engine, exported to destinations including China.
L3Harris Technologies (September 2019)	$13 million, $6.5 million suspended	131 alleged violations, including unauthorized exports of technical data, some in software, and of tactical radios and military electronics, license-proviso violations and a false statement. Harris disclosed most of them voluntarily; the State Department found the others.

Voluntary disclosure did not remove the penalties: GE Aerospace and Boeing disclosed every violation, and BAE Systems all but one, and each agreed to an external Special Compliance Officer.

> **How SecurePoint uses these cases**
>
> None of these cases arose from a facility visit. They involve employees and contractors, company IT systems, drawings sent abroad and the conditions on licenses. SecurePoint cites them to show how DDTC treats technical data that reaches a foreign person, which a visit can also produce, and does not claim that a visitor system would have prevented any of them.

9. An implementation plan

The steps below set the order of the work. How long each takes depends on the number of sites, the controlled areas in each and your security review, and a signed project plan sets the dates.

1. **Scope the program**
   Identify the sites and areas that hold technical data, the U.S. Munitions List categories and export classifications involved, and the visits that could expose them. Confirm whether the NISPOM or a license proviso requires a TCP for any site, and who decides U.S.-person status, export classification and disclosure.

2. **Write the visitor rules into the TCP**
   Who needs a host, an escort, an NDA or an ID check; what a visitor may see along the approved route; how escorts hand over; and what happens when a visitor's status is unresolved.

3. **Configure the visitor system**
   Set each controlled site's rules, the lists you screen against, the review threshold and re-screening interval, and the badge each site prints. Document how escorts and physical access controls enforce the boundaries a visitor system cannot see.

4. **Test with visits of each kind**
   Run test visits for a U.S. citizen, a permanent resident, a foreign national from a country outside § 126.1, a national of a § 126.1 country, and a visitor who matches a list. Check each visit's record, badge and evidence export.

5. **Train, then go live**
   Train the front desk, hosts and escorts on their part, and reviewers on match and status decisions. Run the new process alongside the old one at first, and have counsel review the first evidence export against your records program.

Setting up SecurePoint for an ITAR site

The configuration behind step 3:

- Set each site your TCP covers to the ITAR Controlled or DCSA High Security profile.
- Turn on the DDTC debarred list in screening settings and decide whether a match holds the visit; it is off until enabled.
- Set your review threshold and re-screening interval.
- Load your host directory: every check-in at these sites needs a host.
- Choose how a kiosk handles escorts: the front desk assigns them, or, with autonomous check-in, hosts verify foreign nationals and take escort custody.
- Check that each site's badge template prints the escort, status and zone lines.

Sources and revision history

First published March 2026. Last reviewed November 7, 2026 against the sources below and against SecurePoint's product as it stood that day. The sources are listed for traceability, not as endorsements. Confirm current text with the issuing agency before relying on a citation.

[1] **International Traffic in Arms Regulations (22 CFR parts 120 to 130)**
https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M
Export and deemed export (§ 120.50), release (§ 120.56), U.S. person and foreign person (§§ 120.62 and 120.63), ineligible and debarred persons (§§ 120.16(c) and 127.1(d)), and registrants' records (§ 122.5).

[2] **22 CFR § 126.1: Prohibited exports, imports, and sales to or from certain countries**
https://www.ecfr.gov/current/title-22/section-126.1
The countries subject to a policy of denial, and the duty in § 126.1(e)(2) to inform DDTC immediately of a proposed or actual export to one of them. Syria was removed from § 126.1(d)(1) effective October 1, 2026 (91 FR 62313).

[3] **22 CFR § 127.12: Voluntary disclosures**
https://www.ecfr.gov/current/title-22/section-127.12
A disclosure may be a mitigating factor (§ 127.12(a)); after an incomplete initial notification, a full disclosure is due within 60 calendar days (§ 127.12(c)(1)).

[4] **22 CFR § 127.10: Civil penalty**
https://www.ecfr.gov/current/title-22/section-127.10
Civil maximum per violation of 22 U.S.C. 2778: the greater of $1,271,078 or twice the value of the transaction, as adjusted for inflation at 90 FR 1868 (January 10, 2025).

[5] **OMB Memorandum M-26-11 (April 17, 2026)**
https://www.fec.gov/resources/cms-content/documents/OMB-Memo-Cancellation-of-Penalty-Inflation-Adjustments-for-2026.pdf
Cancelled the 2026 civil penalty inflation adjustments; agencies keep their 2025 amounts. The copy linked is the one the Federal Election Commission publishes.

[6] **22 U.S.C. 2778(c): Criminal violations**
https://www.law.cornell.edu/uscode/text/22/2778
Willful violations: a fine of up to $1,000,000, up to 20 years in prison, or both, per violation.

[7] **15 CFR § 734.13: Export (Export Administration Regulations)**
https://www.ecfr.gov/current/title-15/section-734.13
A release of technology or source code to a foreign person in the United States is a deemed export to the person's most recent country of citizenship or permanent residency (§ 734.13(b)). Release is defined in § 734.15.

[8] **15 CFR § 762.6: Period of retention**
https://www.ecfr.gov/current/title-15/section-762.6
EAR records run five years from the latest of the export, a known reexport or transfer, or the end of the transaction.

[9] **32 CFR § 117.11: Foreign ownership, control, or influence (NISPOM)**
https://www.ecfr.gov/current/title-32/section-117.11
Paragraph (h)(1) requires a Technology Control Plan of contractors cleared under a voting trust, proxy agreement, special security agreement or security control agreement, and of others when the cognizant security agency decides one is appropriate.

[10] **8 U.S.C. 1324b: Unfair immigration-related employment practices**
https://www.law.cornell.edu/uscode/text/8/1324b
Defines the protected individuals the ITAR counts as U.S. persons (§ 1324b(a)(3)), and bars national-origin and citizenship-status discrimination in hiring, recruitment or referral for a fee, and discharge.

[11] **U.S. Department of State: GE Aerospace settlement (April 2026)**
https://www.state.gov/releases/bureau-of-political-military-affairs/2026/04/u-s-department-of-state-concludes-36-million-settlement-resolving-export-violations-by-general-electric-company
$36 million consent agreement, $18 million suspended, resolving 116 voluntarily disclosed alleged violations, including unauthorized exports of technical data to China.

[12] **U.S. Department of State: BAE Systems, Inc. settlement (August 2026)**
https://www.state.gov/releases/bureau-of-political-military-affairs/2026/08/u-s-department-of-state-concludes-36-million-settlement-resolving-export-violations-by-bae-systems-inc-bae
$36 million consent agreement, $18 million suspended, resolving 104 alleged violations, all but one voluntarily disclosed.

[13] **U.S. Department of State: The Boeing Company settlement (February 2024)**
https://2021-2025.state.gov/u-s-department-of-state-concludes-51-million-settlement-resolving-export-violations-by-the-boeing-company/
$51 million consent agreement, $24 million suspended, resolving 199 voluntarily disclosed alleged violations, including unauthorized exports of technical data to foreign-person employees and contractors and to China.

[14] **U.S. Department of State: FLIR Systems, Inc. settlement (April 2018)**
https://2017-2021.state.gov/u-s-department-of-state-concludes-30-million-settlement-of-alleged-export-violations-by-flir-systems-inc/
$30 million consent agreement, $15 million suspended, including unauthorized exports and retransfers of technical data to dual-national employees from Iran, Iraq, Lebanon and Cuba.

[15] **U.S. Department of State: L3Harris Technologies, Inc. settlement (September 2019)**
https://2017-2021.state.gov/u-s-department-of-state-concludes-13-million-settlement-of-alleged-export-violations-by-l3harris-technologies-inc/
$13 million consent agreement, $6.5 million suspended, resolving 131 alleged violations, most voluntarily disclosed.

[16] **U.S. Department of State: Honeywell International, Inc. settlement (announced May 2021)**
https://2021-2025.state.gov/u-s-department-of-state-concludes-13-million-settlement-of-alleged-export-violations-by-honeywell-international-inc/
$13 million consent agreement signed in April 2021, $5 million suspended, resolving 34 voluntarily disclosed alleged violations involving engineering drawings with technical data.

[17] **DDTC Penalties and Oversight Agreements**
https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=384b968adb3cd30044f9ff621f961941
DDTC's index of consent agreements and charging letters.

Revision history

November 7, 2026 Rewritten so the web page and the PDF carry the same text. Added how the EAR counts a visitor’s countries differently from the ITAR, when the NISPOM requires a Technology Control Plan, the § 126.1(e)(2) notice and the timing of a voluntary disclosure, a note on anti-discrimination law, and the badge lines SecurePoint prints at a controlled site. Replaced the workflow phases with a table of what SecurePoint enforces, what it records and what stays with your organization, and removed statements the product does not support: an authorized escort roster, escort data in the after-visit report, logged badge return and deactivation, monitoring of where visitors go, a separation of duties the roles do not enforce, and an implementation timeline nobody had measured. The subtitle no longer says visitor screening meets ITAR requirements.

October 30, 2026 Clarified the scope and trigger of ITAR record retention, left U.S.-person status and license or exemption determinations with the export-control officer or counsel, and distinguished visitor-workflow support from physical TCP enforcement. Removed claims that a visitor's export classification decides their zones, that each zone sets badge permissions, that badges reflect an approved access posture, and that customers configure site zones in SecurePoint; described the zone line SecurePoint badges print; and directed country-policy review to the current rule.

October 23, 2026 Updated the ITAR § 126.1 country examples (Syria came off the list on October 1, 2026; China, Venezuela, and Burma are now named) and added the 2024 and 2026 DDTC consent agreements with Boeing, GE Aerospace, and BAE Systems. Corrected the citations for escorts, zone separation, and records, where SecurePoint captures U.S.-person status, and when check-in screens a visitor again.

October 17, 2026 Corrected ITAR citations and penalty figures, and removed a claim that SecurePoint enforces zone boundaries.

September 27, 2026 Described the DDTC debarred list as off until an administrator enables it, and removed an unmeasured deployment-time figure.

About SecurePoint USA

SecurePoint USA builds visitor management and restricted-party screening software for defense contractors, manufacturers, research facilities and schools. It screens visitors and other parties against government sanctions and restricted-party lists, holds possible matches for a person to decide, issues badges once a site's required evidence is in place, and keeps an append-only, hash-chained audit log that application users cannot edit or delete, with a verifier that checks the chain. SecurePoint does not file with OFAC, BIS or DDTC, and it does not make an organization compliant: it supplies records for the program your organization runs.

See an ITAR visit from check-in to badge.

Request a demo to watch a foreign national check in at a controlled site, a host verify the visit and take escort custody, and the badge print with its escort and zone lines, using demonstration data.

- Request a demo: securepointusa.com/request-demo
- Read this paper online: securepointusa.com/resources/whitepapers/itar-visitor-screening
- All whitepapers: securepointusa.com/resources/whitepapers

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, or by the compliance, security, export-control or assessment professionals familiar with your organization, its 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 product behavior as of the "Last reviewed" date, not a contractual commitment. Capability fit for any specific environment must be confirmed during scoping.

© 2026 SecurePoint USA LLC. All rights reserved.