Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/audit-discovery-preparation/04-export-controls/

AUDIT AND DISCOVERY PREPARATION

EAR and ITAR information gathering package

Gather products, technology, access and transaction facts for an EAR or ITAR export control specialist. Keep classification decisions separate.

Prepare business, item, technology, transaction and access facts for an export control specialist to determine jurisdiction, classification and required authorizations.

Business owners, contract teams, engineering, IT, attorneys and export coordinators

EAR and ITAR preparation with cyber and data handling questions. Sanctions, customs, nuclear exports, classified information and other regimes may require additional specialists.

Before you gather

EAR and ITAR are different export control regimes, each governing exports and their authorizations, and both sit apart from cybersecurity audit certification. Start with the items, the software, the technical information, the services and the transactions, because the specialist determines jurisdiction and classification from those facts, including whether another agency or regime applies. A transaction can involve electronic access, remote support, source code sharing, engineering collaboration or services as well as physical shipments, so gather who may access what, from where, with which permissions and under which authorization. Route person status questions to counsel through a restricted process.

DDTC registration, where required, sits alongside the export authorization for each activity. A supplier label, an old ECCN, an ITAR clause or a cloud marketing statement is input for the specialist's review, and the strongest classification file traces each inherited classification back to a documented decision. Keep the supporting classification, the license, the agreement, the provisos and the change history together as one record.

EAR 734.18 and ITAR 120.54 contain different conditional provisions for certain encrypted transmission and storage, and the current ITAR text reviewed has recent 2026 amendments. Ask the specialist to review the exact current text, the encryption boundary, the authorized recipients, the key control, the locations and the provider access. Recordkeeping periods have different starting events: EAR 762.6 uses five years from the latest specified event and restricts destruction after an agency request, and ITAR 122.5 has its own license, approval and transaction rules with individual variation. Gather the actual dates and hold instructions, and have the specialist set the schedule from the specified starting events.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Give each request to the suggested owner. Record each answer, including the items awaiting confirmation, in the editable CSV checklist. Keep the records themselves in a secure evidence location agreed with the recipient and use the checklist as the index that points to them; passwords stay with their owners, and real patient data and controlled technical information stay in the secure location.

Records to find

CSV files hold plain records, and your spreadsheet sets the layout. Import as UTF-8, keep IDs as text, wrap text and widen columns before use. Blank client fields are intentional.

EX-R01 Entity activities and responsible people

Ask
Business owner

Gather
Legal entities, sites/countries, products, manufacturing, software, research, services, brokering if relevant, customers and export responsibility contacts.

Where to ask
Corporate, engineering and sales records

Why it may be needed
Defines the proposed consultation and possible regimes.

If missing or uncertain
Describe the activity and ask for jurisdiction review, leaving the classification field for the specialist.

Reference: EA01; IT04

EA01 IT04

EX-R02 Item and technology descriptions

Ask
Engineering or product owner

Gather
Part/model/version list, function, performance specifications, materials, source/object code distinctions, drawings, manuals and technical data categories.

Where to ask
Engineering, PLM, repositories and product documentation

Why it may be needed
Provides the facts needed for a qualified jurisdiction/classification decision.

If missing or uncertain
Start with a sanitized description and arrange controlled specialist access before sharing technical data.

Reference: EA01; IT01

EA01 IT01

© 2026 Global Digital Forensics, Inc. All rights reserved.

EX-R03 Existing jurisdiction and classifications

Ask
Export coordinator

Gather
ECCNs, USML categories, EAR99 determinations, commodity jurisdiction/CCATS records if obtained, supplier classifications, rationale, dates and version history.

Where to ask
Export files, suppliers and counsel

Why it may be needed
Shows what was actually determined and which item/version it covers.

If missing or uncertain
Record Not yet determined. Treat a supplier opinion as input that the specialist confirms, distinct from a government determination.

Reference: EA03; EA04; IT04

EA03 EA04 IT04

EX-R04 Transaction map

Ask
Sales and logistics

Gather
Proposed/prior transactions, destinations, parties, intermediaries, end users, end uses, routing, reexports/retransfers and ultimate consignees.

Where to ask
CRM, ERP, shipping and project records

Why it may be needed
Connects item facts to transaction specific review.

If missing or uncertain
Route any open end use or destination question to the specialist before release.

Reference: EA05; EA04; IT04

EA05 EA04 IT04

EX-R05 Authorizations and restrictions

Ask
Export coordinator and counsel

Gather
Licenses, exceptions/exemptions basis, agreements, registrations where applicable, amendments, provisos, expiration dates and authorized parties/sites/data/services.

Where to ask
BIS/DDTC records and signed agreements

Why it may be needed
Allows specialist comparison of actual activity with authorized scope.

Reference: IT03; IT05; EA04

IT03 IT05 EA04

© 2026 Global Digital Forensics, Inc. All rights reserved.

EX-R06 Screening and escalation records

Ask
Compliance and sales

Gather
Screening procedure, dated results, party identifiers, red flags, end use statements, escalation and release approvals, plus screening tool scope.

Where to ask
Screening provider, compliance and sales

Why it may be needed
Supports review of the actual decision at the time of transaction.

Reference: EA05; EA04

EA05 EA04

EX-R07 Technical information locations

Ask
Engineering and IT

Gather
Where technical information lives: design/source repositories, email, Teams/Slack, cloud drives, PLM, ticket systems, backups, removable devices and outside partners.

Where to ask
Data source atlas, engineering and providers

Why it may be needed
Looks for copies and transfers beyond the product shipment.

If missing or uncertain
Hold each location as a candidate until an owner responds.

Reference: EA01; IT01; IT02

EA01 IT01 IT02

EX-R08 Access and support facts

Ask
IT, HR and counsel

Gather
Actual access roles, contractor/provider organizations, work/support locations, foreign person review process, access approvals and permitted remote administration.

Where to ask
Identity, HR, vendor and access records

Why it may be needed
Enables legal review of access/release risk while personal status stays in the restricted counsel file.

If missing or uncertain
Counsel defines lawful, limited verification.

Reference: EA01; IT01; IT02

EA01 IT01 IT02

© 2026 Global Digital Forensics, Inc. All rights reserved.

EX-R09 Cloud and cryptographic facts

Ask
IT architect and provider

Gather
Services/regions, replication, backups, disaster recovery, subcontractors, admin/support access, encryption boundary, module/strength details, key custody and decryption permissions.

Where to ask
Architecture, service contracts and provider security documents

Why it may be needed
Gives the specialist facts for the distinct EAR/ITAR encrypted data provisions.

If missing or uncertain
Where keys, provider access or regions are open, request written technical facts from the provider.

Reference: EA01 734.18; IT02

EA01 IT02

EX-R10 Technology access procedures

Ask
Export coordinator and IT

Gather
Existing technology control plans, permission reviews, visitor/collaboration rules, travel/device processes and exception records.

Where to ask
Export, facilities, IT and engineering

Why it may be needed
Supplies existing measures for specialist review, with implementation records gathered alongside any template.

If missing or uncertain
Label a draft or proposed measure clearly; specialist determines what the activity requires.

Reference: EA03; EA04; IT04

EA03 EA04 IT04

EX-R11 Shipment and electronic release records

Ask
Logistics and system owners

Gather
Orders, invoices, shipment/export declarations where applicable, serial/item versions, authorizations referenced, transfer/access records and delivery acknowledgments.

Where to ask
ERP, freight forwarder, engineering and access logs

Why it may be needed
Links activity, authority and recipient over time.

If missing or uncertain
Identify records controlled by another party, note who holds them and arrange an authorized request.

Reference: EA02; IT03

EA02 IT03

© 2026 Global Digital Forensics, Inc. All rights reserved.

EX-R12 Retention and reproducibility

Ask
Records manager and IT

Gather
Schedules, license/transaction dates, record formats, change history, agency requests/holds, storage/access and ability to reproduce complete readable records.

Where to ask
Export archive, providers and legal holds

Why it may be needed
Enables separate EAR/ITAR schedule and reproduction review.

Reference: EA02 762.6; IT03 122.5

EA02 IT03

EX-R13 Training and business change

Ask
HR and export coordinator

Gather
Role specific training, attendance, policies, changes to product/ownership/country/personnel/providers and prior advice about those changes.

Where to ask
HR, export program and project history

Why it may be needed
Helps the specialist test earlier decisions against current facts.

If missing or uncertain
Record the change and date.

Reference: EA03; IT04

EA03 IT04

EX-R14 Prior review and incident records

Ask
Counsel and export lead

Gather
Previous specialist reports, findings, corrective actions, suspected unauthorized access/shipments, regulator correspondence and disclosure records where authorized.

Where to ask
Restricted counsel/export files

Why it may be needed
Keeps open issues in view and representations consistent with earlier statements.

If missing or uncertain
Send potential violations to counsel and the specialist promptly; counsel determines reportability and handles any disclosure.

Reference: EA04; IT04

EA04 IT04

© 2026 Global Digital Forensics, Inc. All rights reserved.

EX-R15 Secure specialist access

Ask
Business sponsor and counsel

Gather
Identity/authorization of proposed recipients, secure repository, access restrictions, legal agreement and approved transfer method.

Where to ask
Engagement and information security records

Why it may be needed
Sharing the preparation evidence can itself require export and privacy review.

If missing or uncertain
Supply a nonsensitive index until authority and secure delivery are agreed.

Reference: EA01; IT02; IT03

EA01 IT02 IT03

Questions for client IT and owners

A useful answer names the actual system, period, supporting record and its coverage. Where the answer sits with someone else, name the person or provider who can give it.

1. What precisely are you asking the specialist to review: hardware, software, technical data, services or a transaction?

Suggested responder
Client IT or system owner

Useful supporting record
Item/version list and a sanitized activity description.

2. Who made each existing classification and what version and facts did it cover?

Suggested responder
Client IT or system owner

Useful supporting record
Dated rationale and government/supplier correspondence, clearly distinguished.

3. Where can people outside the approved project view, download or administer the information?

Suggested responder
Client IT or system owner

Useful supporting record
Access map including support, backups, ticketing and collaboration.

© 2026 Global Digital Forensics, Inc. All rights reserved.

4. Can any provider, administrator or subprocessor decrypt the information?

Suggested responder
Client IT or system owner

Useful supporting record
Architecture and key custody statement; secrets stay with their owners.

5. Which countries, people and entities are involved in the planned activity?

Suggested responder
Client IT or system owner

Useful supporting record
Restricted transaction/person review file approved by counsel.

6. Which license, agreement, exception or exemption is proposed as the authorization?

Suggested responder
Client IT or system owner

Useful supporting record
Document, provisos, expiration, parties and specialist question.

7. What changed since the previous determination?

Suggested responder
Client IT or system owner

Useful supporting record
Change list covering technology, parties, destinations and services.

8. Are there agency requests, existing holds or prior transfers that need review?

Suggested responder
Client IT or system owner

Useful supporting record
Counsel controlled chronology and records index.

Facts to confirm and specialist decisions

These are explicit handoff questions, and each one closes with the specialist's written answer, drawing on the records marked Received. Add client specific questions and a responsible person.

© 2026 Global Digital Forensics, Inc. All rights reserved.

EX-Q01 Which items/data/services are subject to EAR, ITAR, another regime or a documented exclusion?

Ask
Export control specialist and counsel

Gather
Specifications, jurisdiction/classification history, technical descriptions and activities

Resolution needed
Written determination by the specialist, tied to the actual item/version.

EX-Q02 Is the proposed storage/access/transfer authorized, including provider support and key access?

Ask
Export control specialist with IT architect

Gather
Actual access paths, parties/locations, encryption facts and authorizations

Resolution needed
Transaction and system specific instructions, including any conditions to satisfy before release.

EX-Q03 Which additional sanctions, nuclear, classified or contractual restrictions need separate review?

Ask
Counsel and appropriate specialist

Gather
Parties, countries, products/services and contract

Resolution needed
Explicit referral or documented exclusion, so each further regime gets its own review alongside EAR/ITAR.

Preparing the handoff

The handoff is ready when sanitized entity, activity, item and version descriptions have been supplied first; when confirmed classifications and authorizations are distinguished from proposed classifications and open questions; when the access, cloud, technical data and transaction maps identify their open items and owners; and when the specialist has confirmed authorization before receiving restricted technical information or advising any release.

Sources for this package

Official laws/rules establish duties within their scope. Guidance explains programs; NIST supplies methods; vendor documentation describes possible product behavior. The package works alongside the actual contracts, facts, configuration and case orders.

- EA01 EAR scope
- EA02 EAR recordkeeping

© 2026 Global Digital Forensics, Inc. All rights reserved.

- EA03 BIS export compliance programs
- EA04 BIS export compliance toolkit
- EA05 EAR end user and end use controls
- IT01 ITAR definitions
- IT02 ITAR encrypted technical data provision
- IT03 ITAR registration and recordkeeping
- IT04 DDTC understanding ITAR
- IT05 DDTC registration explanation

These materials help you prepare and gather information for the professional you bring them to. That professional sets the scope, the records and the conclusions with you.

Source review date: October 18 2026.

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.