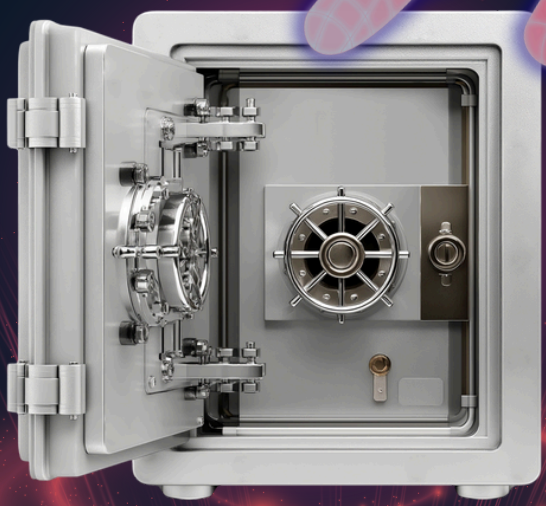
ITAR COMPLIANCE

Cybersecurity & Legal Compliance Self-Check



BREA NETWORKS

BREA NETWORKS
CMMCCOMPLIANCE.US

A PRACTICAL CHECKLIST FOR DEFENSE CONTRACTORS HANDLING ITAR-CONTROLLED DATA

Ensure your organization protects export-controlled data, restricts foreign access, and meets obligations under ITAR (22 CFR Parts 120–130).

Includes

- Core requirements from 22 CFR 120–130
- Registration and licensing obligations
- Data protection and access controls
- Governance and oversight requirements
- Yes / No / Maybe readiness review
- Clear remediation next steps

TABLE OF CONTENTS

INTENDED AUDIENCE

This document is intended for organizations subject to ITAR (22 CFR 120–130), including:

- USML manufacturers
- USML exporters
- ITAR defense service providers
- ITAR technical data controllers
- DDTC registrants (§122)

This framework supports evaluation of ITAR governance, technical safeguards, and regulatory obligations.

ITAR APPLICABILITY DETERMINATION

ITAR jurisdiction (22 CFR 120–130) is triggered by U.S. Munitions List (USML) classification, ITAR-defined technical data, provision of ITAR-controlled defense services, or foreign person access to controlled items or data.

In practice, ITAR applicability is typically identified within contractual language. Prime contracts and subcontracts frequently reference “ITAR (22 CFR 120–130),” DDTC registration requirements, export restrictions, or foreign person limitations.

When ITAR is explicitly referenced in contract terms, the organization is operating under ITAR regulatory obligations.

ITAR COMPLIANCE MATURITY MODEL

ITAR compliance is not a single action or filing. It involves layered legal, organizational, and technical obligations under 22 CFR Parts 120–130.

The U.S. Government does not publish a formal “maturity model” for ITAR compliance. The structure presented here is a conceptual framework developed to illustrate the progression from registration to full operational compliance.

This model organizes ITAR obligations into three practical tiers to clarify scope, complexity, and implementation effort.

Registration is procedural. Governance establishes accountability. Technical defense enforces protection.

Most compliance gaps occur when organizations complete registration but do not advance through governance and technical control implementation.

ITAR COMPLIANCE MATURITY MODEL

MATURITY LEVEL 1: REGISTRATION

Focus: Legal eligibility to handle ITAR-controlled data
Status: Required starting point
Effort: Low

What's Required

- Registration with the U.S. Department of State DDTC
- Annual registration renewal
- Payment of annual registration fee

What This Does Not Do

- Does not secure your systems
- Does not protect ITAR data
- Does not prevent violations

Registration simply puts you on record.
It does not make you compliant in practice.

Difficulty: Low
Estimated Time: Days

ITAR COMPLIANCE MATURITY MODEL

MATURITY LEVEL 2: GOVERNANCE

Focus: Organizational intent, accountability, and policy
Status: Required for operational compliance
Effort: Moderate

What's Required

- ITAR Program Manual developed
- Written policies and procedures
- Executive ownership and accountability
- Formal leadership approval and oversight

Typical Deliverables

- CEO or executive memo
- Board or leadership resolution
- Defined roles and responsibilities
- Documented ITAR compliance program

Governance establishes who is responsible and how decisions are made.

Without this level, technical controls lack authority and consistency.

Difficulty: Moderate
Estimated Time: Weeks

ITAR COMPLIANCE MATURITY MODEL

MATURITY LEVEL 3: TECHNICAL DEFENSE

Focus: Actual protection of ITAR-controlled data
Status: Where real compliance happens
Effort: High

What's Required

- ITAR-aware technology stack
- Secure email and collaboration tools
- Data stored and processed in the United States
- U.S.-person-only access controls
- Endpoint, network, and cloud security
- Encryption at rest and in transit
- Monitoring, logging, and alerting
- Physical security controls
- Ongoing compliance program

This is where ITAR and CMMC Level 2 overlap most heavily.

Most violations occur because organizations never fully reach this level.

Difficulty: Critical / Complex
Estimated Time: Months

ITAR COMPLIANCE MATURITY MODEL

WHY MOST COMPANIES STRUGGLE WITH ITAR

Many organizations:

- Stop after registration
- Rely on informal rules instead of enforced controls
- Use cloud tools not designed for ITAR
- Assume cybersecurity tools alone are enough

ITAR requires people, policy, and technology working together.

Missing any one of these creates risk.

HOW THIS CHECKLIST FITS INTO THE MODEL

This checklist focuses primarily on:

- Maturity Level 2 (Governance)
- Maturity Level 3 (Technical Defense)

It helps you identify:

- Gaps in access control
- Weak documentation
- Technical exposure
- Legal and reporting risks

If you have completed Level 1 only, this checklist will show you what comes next.

ASSESSMENT METHODOLOGY

This document is an internal compliance review tool and does not constitute certification or legal determination.

For each control:

- Validate implementation
- Record compliance status
- Document deficiencies

Evaluation should be based on documented policy, technical configuration, and operational enforcement, not informal practice.

Controls identified as No or Maybe indicate areas requiring remediation or further review.

ITAR CONTROL FRAMEWORK

TECHNICAL SAFEGUARDS

U.S. Person Access Enforcement	Access to ITAR-controlled technical data is restricted to verified U.S. Persons through technical controls.	□ Implemented □ Partial □ Not Implemented
Role-Based Access Control (RBAC)	Access to ITAR systems and data is limited based on defined job roles and least-privilege principles.	□ Implemented □ Partial □ Not Implemented
ITAR Environment Segmentation	ITAR systems and data are logically or physically segmented from non-ITAR environments.	□ Implemented □ Partial □ Not Implemented
Unauthorized Export Prevention Controls	Technical safeguards prevent unapproved transmission, transfer, or sharing of ITAR-controlled data.	□ Implemented □ Partial □ Not Implemented
Automated Data Loss Prevention (DLP)	Automated controls monitor and block unauthorized transmission of ITAR data via email, web, or removable media.	□ Implemented □ Partial □ Not Implemented
Encryption in Transit	ITAR-controlled data is encrypted during transmission using validated cryptographic protocols.	□ Implemented □ Partial □ Not Implemented
Encryption at Rest (Server & Storage)	ITAR-controlled data stored on servers or storage platforms is encrypted.	□ Implemented □ Partial □ Not Implemented

ITAR CONTROL FRAMEWORK

TECHNICAL SAFEGUARDS

Endpoint Full-Disk Encryption	All endpoints accessing ITAR data enforce full-disk encryption using validated cryptography.	□ Implemented □ Partial □ Not Implemented
Removable Media Technical Restrictions	USB and removable storage access is restricted, disabled, or technically controlled on ITAR systems.	□ Implemented □ Partial □ Not Implemented
Media Sanitization Controls	ITAR data is securely erased or destroyed prior to device reuse or disposal.	□ Implemented □ Partial □ Not Implemented
Secure Remote Access Controls	Remote access to ITAR systems is restricted, encrypted, and technically enforced.	□ Implemented □ Partial □ Not Implemented
Split Tunneling Prevention	VPN configurations prevent split tunneling that could expose ITAR data to unsecured networks.	□ Implemented □ Partial □ Not Implemented
Secure Cloud Configuration	Cloud services handling ITAR data are configured to meet jurisdictional, access, and export control requirements.	□ Implemented □ Partial □ Not Implemented
Audit Logging & Activity Monitoring	Access to ITAR systems and data is logged and reviewed.	□ Implemented □ Partial □ Not Implemented

ITAR CONTROL FRAMEWORK

TECHNICAL SAFEGUARDS

Administrative Account Monitoring	Privileged or administrative accounts are monitored and reviewed for anomalous activity.	□ Implemented □ Partial □ Not Implemented
Network Monitoring Controls	Outbound network traffic is monitored for unauthorized data transfer.	□ Implemented □ Partial □ Not Implemented
Malware & File Scanning	Systems handling ITAR data are protected by active malware detection and scanning controls.	□ Implemented □ Partial □ Not Implemented
Secure Backup Controls	Backups containing ITAR data are encrypted and access-restricted.	□ Implemented □ Partial □ Not Implemented
System Hardening Standards	Systems handling ITAR data are configured using defined security baselines and hardening standards.	□ Implemented □ Partial □ Not Implemented

ITAR CONTROL FRAMEWORK

PERSONNEL & ACCESS CONTROLS

Annual ITAR Training	Personnel with access to ITAR-controlled data receive documented annual ITAR training.	□ Implemented □ Partial □ Not Implemented
ITAR Acknowledgment	Personnel formally acknowledge ITAR handling responsibilities prior to access.	□ Implemented □ Partial □ Not Implemented
U.S. Person Verification	U.S. Person status is verified and documented before granting ITAR system access.	□ Implemented □ Partial □ Not Implemented
Foreign Person Access Restriction	Access by foreign persons to ITAR-controlled data is technically and procedurally restricted.	□ Implemented □ Partial □ Not Implemented
Access Authorization Approval	Access to ITAR systems is formally approved prior to provisioning.	□ Implemented □ Partial □ Not Implemented
Role-Based Access Assignment	User access is assigned according to defined job roles and least-privilege principles.	□ Implemented □ Partial □ Not Implemented
Privileged Access Governance	Administrative or elevated access requires documented executive approval.	□ Implemented □ Partial □ Not Implemented

ITAR CONTROL FRAMEWORK

PERSONNEL & ACCESS CONTROLS

Access Change Management	Changes to user roles, privileges, or department assignments are formally controlled.	□ Implemented □ Partial □ Not Implemented
Account Termination Controls	User access is promptly revoked upon termination or role change.	□ Implemented □ Partial □ Not Implemented
Insider Threat Awareness	Personnel are trained to recognize and report insider risk indicators.	□ Implemented □ Partial □ Not Implemented
Adverse Personnel Monitoring	Processes exist to identify behavioral, legal, or foreign influence risks.	□ Implemented □ Partial □ Not Implemented
Multi-Factor Authentication Enforcement	MFA is required for user authentication to ITAR systems.	□ Implemented □ Partial □ Not Implemented
Session Lock & Timeout Controls	User sessions automatically lock or terminate after defined inactivity periods.	□ Implemented □ Partial □ Not Implemented

ITAR CONTROL FRAMEWORK

PHYSICAL SECURITY

Controlled Facility Access	Physical access to ITAR areas is restricted to authorized personnel.	□ Implemented □ Partial □ Not Implemented
U.S. Person Area Restriction	ITAR-controlled areas are restricted to verified U.S. Persons.	□ Implemented □ Partial □ Not Implemented
Visitor Logging & Escort	Visitors are logged, screened, and escorted in ITAR areas.	□ Implemented □ Partial □ Not Implemented
ITAR Area Signage	ITAR-controlled areas are clearly marked with access restrictions.	□ Implemented □ Partial □ Not Implemented
Badge Identification System	Badge controls distinguish U.S. Persons from restricted visitors.	□ Implemented □ Partial □ Not Implemented
Physical Access Logging	Access to ITAR-controlled areas is logged and retained.	□ Implemented □ Partial □ Not Implemented
CCTV Monitoring	ITAR-controlled areas are monitored via surveillance systems.	□ Implemented □ Partial □ Not Implemented

ITAR CONTROL FRAMEWORK

PHYSICAL SECURITY

CCTV Footage Retention	Surveillance footage is retained according to defined policy.	□ Implemented □ Partial □ Not Implemented
NDAA §889-Compliant Equipment	Telecommunications and surveillance equipment complies with NDAA §889 restrictions.	□ Implemented □ Partial □ Not Implemented
Secure ITAR Storage	Physical ITAR documents and media are stored in controlled, locked environments.	□ Implemented □ Partial □ Not Implemented
Alternative Work Site Controls	Off-site or alternate work locations handling ITAR data enforce equivalent safeguards.	□ Implemented □ Partial □ Not Implemented

ITAR CONTROL FRAMEWORK

INCIDENT RESPONSE & REPORTING

ITAR-Specific Incident Response Plan	The organization maintains an incident response plan that addresses ITAR-controlled technical data exposure scenarios.	□ Implemented □ Partial □ Not Implemented
Export Violation Escalation Procedures	Defined procedures exist to escalate suspected ITAR violations to executive leadership and compliance officers.	□ Implemented □ Partial □ Not Implemented
Regulatory Reporting & Disclosure Procedures	Documented procedures exist for evaluating, escalating, and submitting required or voluntary disclosures to the DDTC under ITAR (22 CFR §127).	□ Implemented □ Partial □ Not Implemented
Incident Containment Procedures	Documented procedures exist to isolate affected systems and prevent further unauthorized export.	□ Implemented □ Partial □ Not Implemented
Incident Documentation & Retention	Security incidents involving ITAR data are formally documented and retained.	□ Implemented □ Partial □ Not Implemented
Post-Incident Review & Corrective Action	Incidents involving ITAR data trigger corrective action and control improvements.	□ Implemented □ Partial □ Not Implemented

LEGAL & REGULATORY REQUIREMENTS (22 CFR 120–130)

ITAR Registration	The organization maintains active registration with the Directorate of Defense Trade Controls (DDTC) in accordance with 22 CFR §122.	□ Implemented □ Partial □ Not Implemented
Export Licenses	Valid export licenses are obtained and maintained for USML-controlled defense articles and technical data in accordance with 22 CFR §123.	□ Implemented □ Partial □ Not Implemented
Technical Assistance Agreements (TAA)	Technical Assistance Agreements are executed and maintained when providing defense services or authorizing foreign person access under 22 CFR §124.	□ Implemented □ Partial □ Not Implemented
Third-Party Flow-Down Clauses	Contracts with vendors, subcontractors, and partners include appropriate ITAR flow-down and export control clauses.	□ Implemented □ Partial □ Not Implemented
ITAR Recordkeeping (Five-Year Retention)	Export-related records are retained for a minimum of five years in accordance with 22 CFR §122.5.	□ Implemented □ Partial □ Not Implemented

SCORING INTERPRETATION

Organizations handling ITAR-controlled technical data are responsible for safeguarding that information in accordance with U.S. export control regulations (22 CFR 120–130).

This framework is designed to help leadership evaluate exposure across technical, personnel, physical, incident response, and regulatory domains.

Interpreting Your Results

Mostly “Implemented”
Core safeguards are in place. Continued validation, monitoring, and governance oversight are required.

Mix of “Implemented” and “Partial”
Controls may exist but lack consistency, documentation, or enforcement. Exposure risk remains.

Multiple “Not Implemented” Responses
The organization may face regulatory, contractual, or legal risk. Immediate remediation planning is recommended.

Items marked “Partial” or “Not Implemented” represent areas requiring executive review and prioritized action.

RECOMMENDED ACTIONS

If you have not already completed CMMC Level 2, start there.

CMMC Level 2 provides the cybersecurity foundation required to properly protect ITAR-controlled data.

👉 **Download our CMMC Level 2 Readiness Checklist**
Understand the full set of cybersecurity practices required before assessment.

If you are already working toward compliance or need help closing gaps:

👉 **Schedule a Compliance Strategy Call**
Review your ITAR and CMMC posture with a compliance expert and get clear next steps.

IMPORTANT NOTE

This checklist is for educational and planning purposes only. It does not constitute legal advice or a compliance determination.

ITAR and CMMC requirements may vary based on contracts, data types, and organizational structure.

You are responsible for protecting controlled data.
This checklist helps you start that process with clarity and confidence.