



# ITAR Compliance and Secure Data Management: Challenges and XQ Solutions

8/10/25



# Executive Summary

The **International Traffic in Arms Regulations (ITAR)**, codified under 22 CFR Parts 120-130, mandate strict controls over the handling of defense-related technical data.

This includes **data sovereignty, encryption, access restrictions, and recordkeeping** requirements, with explicit definitions of what constitutes a “release” of technical data (22 CFR § 120.56), exemptions for certain activities when using end-to-end encryption (22 CFR § 120.54), and detailed obligations for registrants to maintain records (22 CFR § 122.5).

Non-compliance can result in severe legal, financial, and national security consequences, including civil and criminal penalties under the Arms Export Control Act (22 U.S.C. 2778). Violations (22 CFR § 127.11) can result in severe legal, financial, and national security consequences, but the regulations also provide a pathway for **voluntary disclosure** (22 CFR § 127.12) to mitigate penalties when organizations self-report.

To address these requirements, organizations must implement comprehensive security architectures aligned with established frameworks including NIST SP 800-53 Rev. 5, FedRAMP High, DoD Impact Level 5/6, and NIST SP 800-171.

XQ's Zero Trust Data Security Platform provides an automated and modular approach to these challenges through external key management, granular access controls, real-time monitoring capabilities and immutable recordkeeping, enabling organizations to achieve and maintain ITAR compliance while preserving operational efficiency.



# Key Compliance Challenges and XQ Solutions

## 1. Data Sovereignty, Access Control, and “Release” Definition

### Regulatory References:

- 22 CFR § 120.33 (Technical Data Definition)
- 22 CFR § 120.39 (Export Definition)
- 22 CFR § 126.1 (General Prohibitions)
- 22 CFR § 120.56 defines a “release” as any visual inspection, oral/written exchange, or access provision that enables a foreign person to view or possess unencrypted technical data, whether in the U.S. or abroad.
- NIST SP 800-53 Rev. 5 Controls: AC-3 (Access Enforcement), AC-6 (Least Privilege), SC-12 (Cryptographic Key Establishment and Management)

**Requirements:** ITAR-controlled technical data must be accessible only to U.S. persons as defined in 22 CFR § 120.62, and must remain within U.S. territorial boundaries unless specifically authorized for export under an approved license or exemption. Providing access information to enable viewing of unencrypted ITAR data is also considered a release.

### Challenges:

- Preventing unauthorized access by foreign nationals or non-U.S. persons
- Implementing robust identity verification and continuous vetting processes
- Enforcing geographic and network-based access restrictions exclusively to U.S. persons in U.S. territory
- Enabling secure collaboration without inadvertent export violations
- Avoiding accidental exposure via misconfigured cloud or network services

### XQ Solutions:

- GPS/network-based geofencing with real-time location verification
- Multi-layered Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)
- Authentication and continuous identity validation
- Dynamic access revocation capabilities
- Policy-based prevention of access information disclosure to unauthorized individuals

## 2. Cloud Provider Compliance & Data Isolation



## Regulatory References:

- 22 CFR § 120.54(a)(5) & (b) state that sending, storing, or moving ITAR technical data is not an “export” if it is unclassified, secured with end-to-end encryption, and uses FIPS 140-2/3-compliant cryptographic modules.
- 22 CFR § 120.54(c) confirms that mere access to encrypted data under these conditions is not a release or export.
- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)
- DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)
- FedRAMP High Authorization Requirements
- DoD Cloud Computing Security Requirements Guide (SRG) for Impact Levels 5 and 6
- NIST SP 800-171 Rev. 2 (Protecting Controlled Unclassified Information)

**Requirements:** ITAR-controlled data must reside in cloud environments that meet or exceed FedRAMP High authorization requirements and maintain physical presence within U.S. borders. Cloud service providers must meet security requirements “equivalent” to the FedRAMP Moderate baseline as a minimum standard.

End-to-end encryption means the data remains encrypted from the originator’s in-country security boundary to the recipient’s in-country security boundary, with no decryption keys provided to third parties.

## Challenges:

- Selecting ITAR-compliant cloud services that meet FedRAMP High or DoD IL5/IL6 standards
- Ensuring complete data isolation from non-compliant infrastructure
- Managing vendor lock-in risks while maintaining compliance
- Monitoring cloud provider security posture changes
- Ensuring encryption implementation meets FIPS and NIST criteria
- Guaranteeing encryption keys are never exposed to non-U.S. persons or non-compliant jurisdictions

## XQ Solutions:

- Native integration with AWS GovCloud, Microsoft Azure Government, and Google Cloud Assured Workloads
- Automated Virtual Private Cloud (VPC) segregation and network isolation
- Real-time compliance monitoring and automated attestation
- External key management with customer-controlled encryption keys stored in U.S.-based locations
- Automatic application of end-to-end encryption with policy verification before data is stored or transmitted

## 3. Zero Trust Security Architecture Implementation

### Regulatory References:



- 22 CFR § 120.56
- NIST SP 800-207 (Zero Trust Architecture)
- NIST SP 800-53 Rev. 5 Controls: AC-17 (Remote Access), AC-19 (Access Control for Mobile Devices), SC-7 (Boundary Protection)
- Executive Order 14028 (Improving the Nation's Cybersecurity)

**Requirements:** Traditional perimeter-based security models are insufficient for ITAR compliance. Zero Trust principles must be implemented to verify every access request regardless of network location or user credentials.

While ITAR does not prescribe specific Zero Trust architectures, compliance with 22 CFR § 120.56 requires that no technical data be “released” without authorization, making continuous verification a necessity.

#### **Challenges:**

- Eliminating implicit trust and implementing continuous verification
- Preventing lateral movement across network segments
- Maintaining user productivity while enforcing strict access controls
- Scaling verification processes across distributed environments
- Dynamically adjusting access permissions based on threat level
- Maintaining compliance in hybrid and edge computing environments

#### **XQ Solutions:**

- Continuous identity, device, and behavioral verification
- Micro-segmentation of sensitive data stores
- Risk-based adaptive access control with real-time threat assessment
- Session-based access tokens with automatic expiration

## **4. Encryption & Cryptographic Controls**

#### **Regulatory References:**

- FIPS 140-2/140-3 (Cryptographic Module Validation)
- 22 CFR § 120.33 (Technical Data encryption requirements)
- 22 CFR § 120.54(a)(5) requires FIPS 140-2/3-compliant cryptography for exemption from export classification.



- NIST SP 800-53 Rev. 5 Controls: SC-12 (Cryptographic Key Establishment), SC-13 (Cryptographic Protection), SC-28 (Protection of Information at Rest)
- NIST SP 800-57 (Cryptographic Key Management)

**Requirements:** All ITAR-controlled data must be encrypted using FIPS 140-2 or higher validated cryptographic modules for both data at rest and data in transit. Keys must be managed to ensure no unauthorized party can decrypt the data.

**Challenges:**

- Implementing FIPS-validated cryptographic solutions
- Managing large-scale secure key generation, distribution, rotation, and revocation
- Minimizing encryption overhead and performance impact bottlenecks
- Preparing for post-quantum cryptographic transition
- Preventing insider threats with access to cryptographic material

**XQ Solutions:**

- Automated External Key Management (EKM) to generate, store, and rotate keys with FIPS 140-2 Level 3+ validation
- End-to-end zero-knowledge encryption architecture
- Automated external key lifecycle management and rotation
- Quantum-resistant algorithm integration and migration planning
- Zero Trust Data encryption so XQ and cloud providers cannot access plaintext data
- Quantum-resistant algorithms for long-term compliance and future threat mitigation

## 5. Continuous Monitoring & Audit Requirements

**Regulatory References:**

- NIST SP 800-53 Rev. 5 Controls: AU-2 (Event Logging), AU-6 (Audit Record Review), AU-11 (Audit Record Retention), SI-4 (System Monitoring)
- 22 CFR § 126.1(e) (Incident reporting requirements)
- 22 CFR § 122.5
- DFARS 252.204-7012(c) (Incident reporting to DIBNet)



**Requirements:** Organizations must maintain comprehensive, tamper-proof audit logs and implement continuous monitoring for all ITAR data access and processing activities.

- 22 CFR § 122.5 requires registrants to maintain records of manufacturing, acquisition, disposition, export documentation, technical data, and defense services for at least five years from the expiration of licenses or date of transaction.
- Records must be legible, readable, tamper-evident, and readily accessible for inspection.

**Challenges:**

- Managing large volumes of audit data in immutable form while maintaining searchability
- Implementing real-time anomaly detection and threat hunting
- Preventing unauthorized alterations to historical records
- Ensuring log integrity and non-repudiation for compliance audits
- Correlating events across distributed systems and environments
- Maintaining searchable, legible archives over multi-year retention periods

**XQ Solutions:**

- Integrated Security Information and Event Management (SIEM) with Security Orchestration, Automation and Response (SOAR) capabilities
- Immutable audit log storage with cryptographic integrity verification
- Real-time alerting and automated incident response workflows
- Immutable logging with write-once storage
- Granular audit trails for every access and modification event
- Secure, searchable electronic records that meet ITAR's legibility and change-tracking requirements

## 6. Incident Response & Regulatory Reporting

**Regulatory References:**

- 22 CFR § 126.1(e) (Notification requirements for violations)
- DFARS 252.204-7012(c) (Cyber incident reporting to DIBNet)
- NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide)
- 22 CFR § 127.11
- 22 CFR § 127.12



**Requirements:** Security incidents involving ITAR-controlled data must be reported to the U.S. Department of State's Directorate of Defense Trade Controls (DDTC) and the Defense Industrial Base Collaborative Information Sharing Environment (DIBNet) within 72 hours of discovery.

22 CFR § 127.11 outlines penalties for ITAR violations, including civil fines, criminal prosecution, and debarment.

22 CFR § 127.12 allows for voluntary disclosures of violations, which may mitigate penalties if promptly and thoroughly reported.

### **Challenges:**

- Rapid incident detection and initial response
- Structured incident response aligned with regulatory timelines
- Coordinating with multiple government agencies and stakeholders
- Maintaining evidence integrity for potential enforcement actions

### **XQ Solutions:**

- Pre-configured incident response playbooks aligned with ITAR requirements
- Automated regulatory reporting workflows with template generation
- Forensic evidence preservation and chain of custody management

## **XQ: Purpose-Built ITAR Compliance Platform**

### **Core Security Capabilities**

**External Key Management System:** Organizations maintain complete control and ownership of encryption keys through dedicated key repositories that remain logically separate from cloud content infrastructure.



**Zero-Knowledge Encryption Architecture:** Multi-layered encryption ensures that only authorized parties can decrypt content, preventing both XQ and cloud service providers from accessing sensitive data.

**Dynamic Access Control:** Attribute-Based Access Control (ABAC) implementation provides context-aware access decisions based on user identity, device posture, geographic location, time of access, and real-time risk assessment.

**Data Leash Technology:** Enables remote access revocation and automatic rights expiration, allowing organizations to maintain control over data even after it has been shared or distributed.

**Comprehensive Monitoring and Analytics:** Real-time visibility into data access patterns, user behavior, and system activities with forensic-grade audit trails and automated compliance reporting.

**Regulatory Compliance Automation:** Pre-configured policy templates and automated assessments for NIST SP 800-53, NIST SP 800-171, ITAR, CMMC 2.0, and GDPR requirements.

**Performance Optimization:** High-performance encryption and access control implementation with less than 5% system overhead and sub-second access decision processing.

## **XQ Compliance Statement: ITAR & End-to-End Encryption Requirements**

### **Reference:**

*International Traffic in Arms Regulations: Creation of Definition of Activities That Are Not Exports, Reexports, Retransfers, or Temporary Imports; Federal Register Vol. 85, No. 3, Page 70889, Final Rule Published January 2, 2020*

[Link to Official Federal Register Entry](#)

### **Overview:**



In accordance with recent amendments to the International Traffic in Arms Regulations (ITAR), the U.S. Department of State explicitly states that **unclassified technical data secured with compliant end-to-end encryption is not considered an export, reexport, or retransfer** under ITAR. Specifically, **Section 120.52(a)(5)** clarifies that storing, transmitting, or accessing such encrypted data across borders does **not constitute export activity**, provided that certain technical conditions are met.

---

## XQ's Compliance with ITAR Non-Export Definition

XQ's platform—including **XQ Secure Email**, **XQ Transfer**, and **XQ Vault**—**meets and exceeds the ITAR encryption criteria**, thereby ensuring that ITAR-controlled unclassified technical data is treated in compliance with 22 CFR § 120.52(a)(5).

### 1. End-to-End Encryption

XQ applies **end-to-end encryption** to all messages and data payloads. Each file or message is encrypted **on the sender's device**, using a unique symmetric key, and remains encrypted **in transit, at rest, and in use** until decrypted by an authorized recipient.

### 2. FIPS 140-2-Compliant Cryptographic Modules

XQ uses cryptographic libraries and modules that are either:

- **FIPS 140-2 validated**, or
- Implement cryptographic primitives that provide equivalent or greater **security strength** than AES-128, such as **AES-256 GCM** for message payloads and **ECC-based asymmetric key exchange**.

### 3. Secure Key Management

XQ operates a **federated key management model**:

- All encryption keys are managed **externally to cloud storage or transmission systems**, and
- Access to decryption keys is governed by **granular access policies**, including **geofencing, device, role, and identity controls**.



This approach aligns with **NIST SP 800-57** and **NIST SP 800-175B Rev.1** guidance on key management and cryptographic control implementation.

#### 4. Geofencing and Access Controls

XQ supplements encryption with real-time policy enforcement, ensuring that access to ITAR data is only permitted:

- From approved **geographic jurisdictions**,
- By authenticated users with the appropriate **clearances and roles**, and
- On **authorized devices**.

---

### Summary

By satisfying the criteria defined under **22 CFR § 120.52(a)(5)**, the use of XQ to send, store, or access ITAR technical data qualifies as an **activity that is not considered an export, reexport, or retransfer** under U.S. law. This allows defense contractors, research institutions, and federal partners to confidently use XQ for **ITAR-compliant collaboration across distributed cloud environments**, without triggering unintended export violations.

### Integration and Deployment

**Cloud-Native Architecture:** Native support for government cloud environments including AWS GovCloud (US), Microsoft Azure Government, and Google Cloud Assured Workloads.

**Hybrid Environment Support:** Seamless integration across on-premises, cloud, and hybrid infrastructure with consistent security policy enforcement.

**API-First Design:** Comprehensive REST API and SDK support for integration with existing enterprise systems and custom applications.



# Implementation Roadmap

## Phase 1: Assessment and Planning (Weeks 1-4)

- Conduct comprehensive ITAR compliance gap analysis
- Identify current data flows and access patterns
- Develop implementation timeline and resource requirements
- Establish baseline security metrics and KPIs

## Phase 2: Core Infrastructure Deployment (Weeks 5-12)

- Deploy XQ security platform in government cloud or equivalent environment such as the AWS Trusted Secure Enclave
- Implement external key management system
- Configure identity and access management integration
- Establish monitoring and logging infrastructure

## Phase 3: Data Migration and Protection (Weeks 13-20)

- Migrate ITAR-controlled data to compliant environment
- Implement encryption and access controls
- Configure automated compliance monitoring
- Conduct initial security testing and validation

## Phase 4: Operational Integration (Weeks 21-24)

- Deploy DevSecOps pipeline integration
- Implement incident response procedures
- Conduct staff training and certification
- Perform final compliance validation and certification

## Conclusion

ITAR compliance demands a comprehensive security approach that addresses evolving regulatory requirements, mitigates both insider and nation-state threats, and enables secure data governance across complex enterprise environments. XQ's Zero Trust platform provides the technical foundation necessary to meet these stringent requirements while maintaining operational efficiency.

Through the integration of externalized key management, continuous monitoring, quantum-ready encryption, and automated compliance enforcement, XQ enables defense industrial base organizations to:



- Secure ITAR-controlled data across hybrid cloud and on-premises environments
- Reduce audit risk and operational overhead through automation
- Future-proof security infrastructure against emerging threats and regulatory changes
- Maintain competitive advantage while ensuring national security compliance

XQ represents the essential security layer for modern ITAR compliance, providing the technical controls and operational capabilities necessary to protect America's most sensitive defense technologies while enabling innovation and collaboration within the defense industrial base.

---

*This document serves as a technical overview of ITAR compliance requirements and XQ's security solutions. Organizations should consult with qualified legal counsel and compliance experts to ensure full regulatory compliance based on their specific operational requirements and regulatory obligations.*

## References

- **Federal Acquisition Regulation (FAR)**. 2016. "Basic Safeguarding of Covered Contractor Information Systems." 48 CFR § 52.204-21. <https://www.acquisition.gov/far/52.204-21>.
- **Defense Federal Acquisition Regulation Supplement (DFARS)**. 2016. "Safeguarding Covered Defense Information and Cyber Incident Reporting." 48 CFR § 252.204-7012. <https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm>.
- **National Institute of Standards and Technology (NIST)**. 2020. *Security and Privacy Control Baselines for Federal Information Systems and Organizations*. NIST Special Publication 800-53B. <https://csrc.nist.gov/publications/detail/sp/800-53b/final>.



- Microsoft, "Understanding Compliance Between Commercial, Government, DoD & Secret Offerings," Microsoft Tech Community. <https://techcommunity.microsoft.com/blog/publicsectorblog/understanding-compliance-between-commercial-government-dod--secret-offerings---f/4225436>
- **International Traffic in Arms Regulations: Creation of Definition of Activities That Are Not Exports, Reexports, Retransfers, or Temporary Imports; Creation of Definition of Access Information; Revisions to Definitions of Export, Reexport, Retransfer, Temporary Import, and Release**

<https://www.federalregister.gov/d/2019-27438/page-70889>

- Activities that are not exports, reexports, retransfers, or temporary imports
  - "5) Sending, taking, or storing technical data that is:
    - (i) Unclassified;
    - (ii) Secured using end-to-end encryption;
    - (iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES-128);"

