arena

SECURE PRODUCT DEVELOPMENT FOR AEROSPACE AND DEFENSE

DEMONSTRATING ITAR, EAR, AND CMMC COMPLIANCE TO GAIN MARKET ADVANTAGE

ptc

E-BOOK

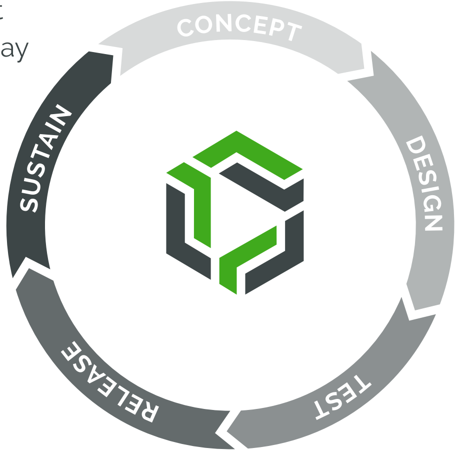
INTRODUCTION

The defense and aerospace market beckons many product companies seeking to diversify, but also demands quality, enhanced efficiencies, technological innovation, and regulatory compliance. Most companies in this market are subject to export controls and cybersecurity regulations, requiring compliance in technical data handling and access. Regulations include the International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and Cybersecurity Maturity Model Certification (CMMC). Their goal is to protect U.S. national security and foreign policy interests.

To mitigate compliance risks and avoid costly legal penalties, companies must ensure the secure access and handling of product information throughout the entire lifecycle. In the past, some manufacturers expressed uncertainty as to whether cloud solutions could address these needs and truly meet regulatory requirements. However, recent initiatives like the Federal Cloud Computing Strategy – Cloud Smart and the United States Department of Defense Digital Engineering Instruction (DoDI 5000.97) are driving organizations to embrace a digital transformation and rethink cloud technology.

Now, leading companies find that a secure cloud-native product lifecycle management (PLM) solution can fully support ITAR, EAR, and CMMC compliance and adds a wide array of other tangible benefits for their businesses.

Arena PLM for AWS GovCloud is the secure product development solution for regulated companies requiring a proven cloud platform designed for their business processes.



INSIDE THIS E-BOOK

- Key Business Considerations for ITAR, EAR, and CMMC Compliance
- Opportunities and Challenges of Defense Market Entry
- A Macro View of Product Lifecycle Management
- What ITAR/EAR/CMMC Means for Secure Product Development
- The Newfound Benefits of Secure Cloud-Native PLM
- How Arena Achieves ITAR/EAR/CMMC Compliance and Business Objectives
- The Path to Secure Product Development and Innovation

KEY BUSINESS CONSIDERATIONS FOR ITAR, EAR, AND CMMC COMPLIANCE

ITAR and EAR

ITAR compliance applies to any entity in the United States that manufactures, sells, distributes, exports, or temporarily imports defense articles, services, or related technical data. These entities span the entire supply chain—from wholesalers, distributors, and vendors to contractors and third-party suppliers.

The items regulated under ITAR are defined in the United States Munitions List (USML)[1]. Product categories include:

- Firearms and ammunition
- Military vehicles
- Aircraft and associated equipment
- Spacecraft systems

Associated technical data, software, and defense services are defined for each product category. Services encompass design, development, testing, repair, and maintenance.

While ITAR regulates defense-related articles, EAR regulates the manufacture, sale, distribution, and export of dual-use items, commercial goods, technology, and data. Dual-use items that have both commercial and military applications, as well as items intended only for commercial use, are outlined in EAR's Commerce Control List (CCL)[2]. Product categories include:

- Electronics
- Computers
- Telecommunications
- Sensors and lasers
- Navigation and avionics
- Marine
- Aerospace and propulsion

FAST FACTS ON ITAR

The United States Munitions List (USML) defines and details the items and services subject to ITAR across 21 different categories.

In order for data to be subject to ITAR, an IT workload or type of data has to be deemed an export according to the USML.

ITAR and EAR impact not only direct holders of defense-related federal contracts, but also subcontractors and wider supply chain stakeholders.

Companies must register for export licenses through the U.S. Department of State Directorate of Defense Trade Controls (DDTC)[3] and the U.S. Department of Commerce's Bureau of Industry and Security (BIS)[4] to be ITAR and EAR compliant. As part of the registration, manufacturers define the type of product information that is under export control. This could include component descriptions, engineering drawings, specifications, test procedures, and bills of materials (BOMs). Regulated data must be controlled and not exported outside the U.S. or accessible to any non-U.S. citizen at any point during design, production, or sustaining activities unless covered under the export license.

CMMC

CMMC compliance applies to U.S. Department of Defense (DoD) contractors, subcontractors, and suppliers. Most small to midsize defense manufacturers must be CMMC-certified once the new ruling goes into effect[5].

The CMMC model is derived from National Institute of Standards and Technology (NIST) and Defense Federal Acquisition Regulation Supplement (DFARS) guidelines—primarily NIST SP 800-171 and DFARS 252.204-7012. Certification requirements are divided into three levels based on the organization's cybersecurity maturity and type of information they handle. Level 1 certification applies to companies handling Federal Contract Information (FCI), whereas Level 2 and 3 certifications apply to companies handling Controlled Unclassified Information (CUI). DoD contractors that use enterprise cloud solutions to handle this information must ensure that the cloud service providers have Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline or Equivalent level security in place.

CMMC Certification Levels

	Requirements	Information Type	Assessment
Level 3 Expert	**110+** cybersecurity practices based on NIST SP 800-171 **24** select practices from NIST SP 800-172 **FedRAMP Moderate** security measures when using a cloud service provider	CUI for high-priority programs	Triennial government-led assessment and annual attestation
Level 2 Advanced	**110** cybersecurity practices aligned with NIST SP 800-171 **FedRAMP Moderate** security measures when using a cloud service provider	CUI	Triennial third-party assessment and annual attestation
Level 1 Foundational	**15** cybersecurity practices based on FAR 52.204-21 **FedRAMP Moderate** security measures when using a cloud service provider	FCI	Annual self-assessment and attestation

HIGH-LEVEL MATURITY ↑ LOW-LEVEL MATURITY

FCI AND CUI EXPLAINED

Federal Contract Information (FCI) is not intended for public release. It is used to develop or deliver a product or service to the government.

Controlled Unclassified Information (CUI) is government-created or owned unclassified information that requires safeguarding and dissemination controls pursuant to applicable laws, regulations, and policies.

LEARN MORE

CMMC Compliance: Key Product Development Considerations for Defense Manufacturers

FedRAMP-Compliant Cloud Solutions Boost Data Security for Aerospace and Defense Manufacturers

OPPORTUNITIES AND CHALLENGES OF DEFENSE MARKET ENTRY

Entering defense-related markets can be enticing and beneficial for product companies, especially for those that originated in commercial markets. Realizing an overall lift from defense market entry, however, depends largely on how well an organization can manage and adhere to the market's regulatory requirements and address the ancillary operational challenges that arise.

Defense spending in the United States is projected to reach $886 billion by 2025[6]

CHALLENGES

Divided Attention

Balancing regulated and commercial product development concurrently can divide attention and divert resources.

New Concerns

ITAR/EAR and CMMC compliance commands new and incremental attention to many product development elements (policies, processes, systems, data classification, and people).

Fluctuating Requirements

Defense customers and prime contractors may demand or modify their own compliance measures at any time as part of flow-down requirements.

OPPORTUNITIES

Reduced Risk

Diversifying beyond traditional commercial offerings can reduce market risk and support growth objectives.

Higher Value Customers

ITAR/EAR-registered and CMMC-certified companies see potential for larger volume sales to single customers with longer product life and service revenue.

Expanded Market Opportunities

Promoting ITAR/EAR and CMMC adherence can make it easier to gain contracts with allied foreign agencies.

A MACRO VIEW OF PRODUCT LIFECYCLE MANAGEMENT (PLM)

Overall, product development has rapidly shifted to meet changing customer demands, increased competition, and more stringent regulations. Companies have responded with smarter and more connected products, lean but highly productive distributed teams, and global best-of-breed partners.

The challenge? How to effectively manage these new complexities.

A big part of the answer is to ensure complete connection and full visibility throughout new product development and introduction (NPDI) and beyond. That means linking all product development, quality activities, and change processes to the complete product record for one's entire team and supply chain partners in a single, reliable view.

Complying with ITAR, EAR, and CMMC won't get businesses to where they want to go if they don't also optimize their approach to product lifecycle management.

Realize the Full Benefits of PLM

STREAMLINE DEVELOPMENT

One Secure Place

☑ Confident Design Control

ADVANCE QUALITY

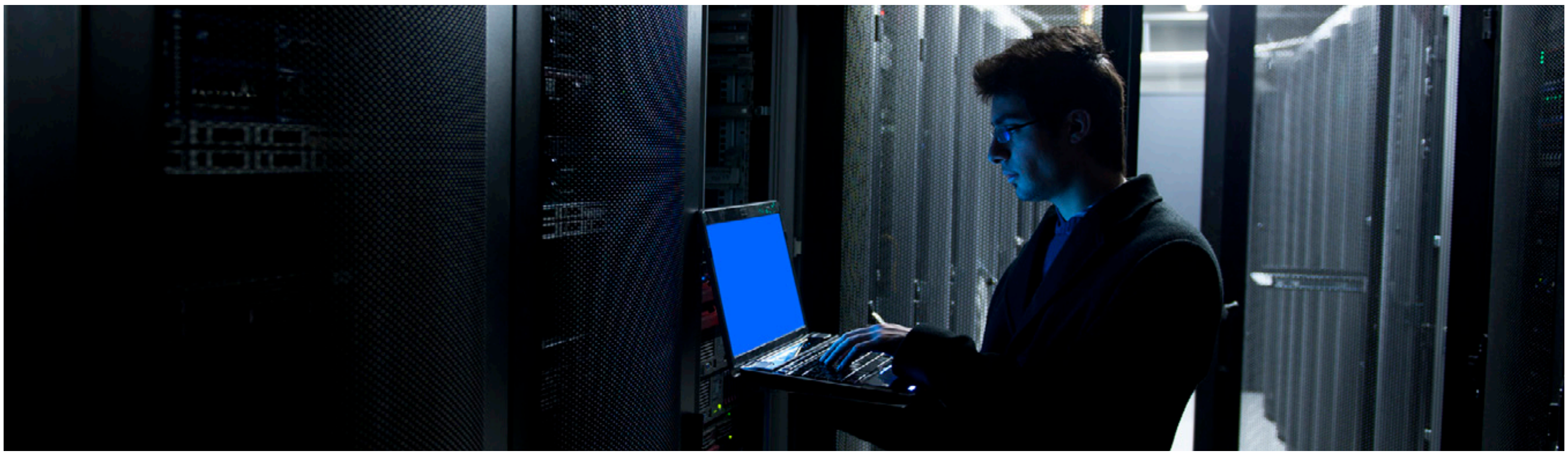
Cross-Functional Traceability

☑ Full Team Collaboration

DRIVE INNOVATION

Strategic Goal Execution

☑ Market Advantage



WHAT ITAR/EAR/CMMC MEANS FOR SECURE PRODUCT DEVELOPMENT

To support ITAR/EAR/CMMC-compliant product development, manufacturers need to adopt measures that ensure technical data and technology—including identified product information—remain accessible where allowed and needed while protecting against loss or unauthorized access. Individual needs and requirements will vary by organization, but generally span three areas.

Data Location

ITAR- and EAR-regulated data must remain in the specified geographic location: the United States. Public commercial cloud services may not meet these requirements, as data can reside in non-U.S. locations or cross geographic borders during transit. While on-premises systems certainly meet geographic location restrictions, such solutions also may not provide team-empowering, traceable ways to collaborate on product development.

Cybersecurity Protections

Systems handling ITAR/EAR/CMMC data should adhere to standards and best practices for ongoing management, monitoring, and review of the multiple security layers (physical, infrastructure, and application). Other needed protections include levels of encryption for in-transit and at-rest data. On-premises solutions may or may not provide these protections, depending upon variables of systems, networks, policy definitions, and IT practices. Some commercial cloud offerings, either public or private, do not necessarily provide these protections.

Companies using commercial cloud solutions must ensure that their cloud service provider has FedRAMP Moderate Baseline or Equivalent level security in place to meet CMMC requirements.

Proper cybersecurity measures encompass:

- Documented plans, policies, and procedures for addressing system security controls, incidence response, and risk mitigation
- User access controls to ensure that only authorized individuals (both internal and external) have access to sensitive product information
- Continuous monitoring for system weaknesses and assessment of security control effectiveness
- Training for employees and external partners on how to mitigate cybersecurity risks, handle sensitive product information, and respond to security breaches

Sophisticated Access Management

Manufacturers must consider data classification and user access since not all product data will be subject to ITAR, EAR, or CMMC. Backend access to the PLM platform must be controlled and restricted to U.S. persons only for ITAR/EAR compliance. Most commercial cloud solutions do not provide these controls; compliance of on-premises solutions depends on the product company's IT resources, physical server location configuration and access, and controlled network security layers.

Manufacturers need the ability to easily identify the technical data that must be ITAR/EAR compliant, and therefore limit access to specific individuals while conversely providing for less-limited access to non-ITAR/EAR technical data. Additionally, companies need visibility of who has accessed sensitive data and when they accessed it.

THE NEWFOUND BENEFITS OF SECURE CLOUD-NATIVE PLM

In the past, managing access to technical data within “four walls” via on-premises server environments was enticing because of technical simplicity and data proximity assurances. What these approaches sacrifice is the essential foundation companies need to move beyond compliance and consistently exceed customer commitments.

DoD contracts, while important, may represent only part of a company's product portfolio. These businesses need more than secure design control and compliance. They need the agility and visibility modern PLM systems provide for cost controls, high quality, and long-term product serviceability for all product offerings (commercial and regulated).

A secure best-in-class cloud-native PLM solution gives manufacturers the complete package—a competitive advantage for all product lines plus the required platform elements for ITAR/EAR/CMMC compliance.

In 2018, the United States Office of Management and Budget further updated its Cloud First strategy with Cloud Smart additions that encourage migration to cloud architecture. Learn more

SECURE DEVELOPMENT

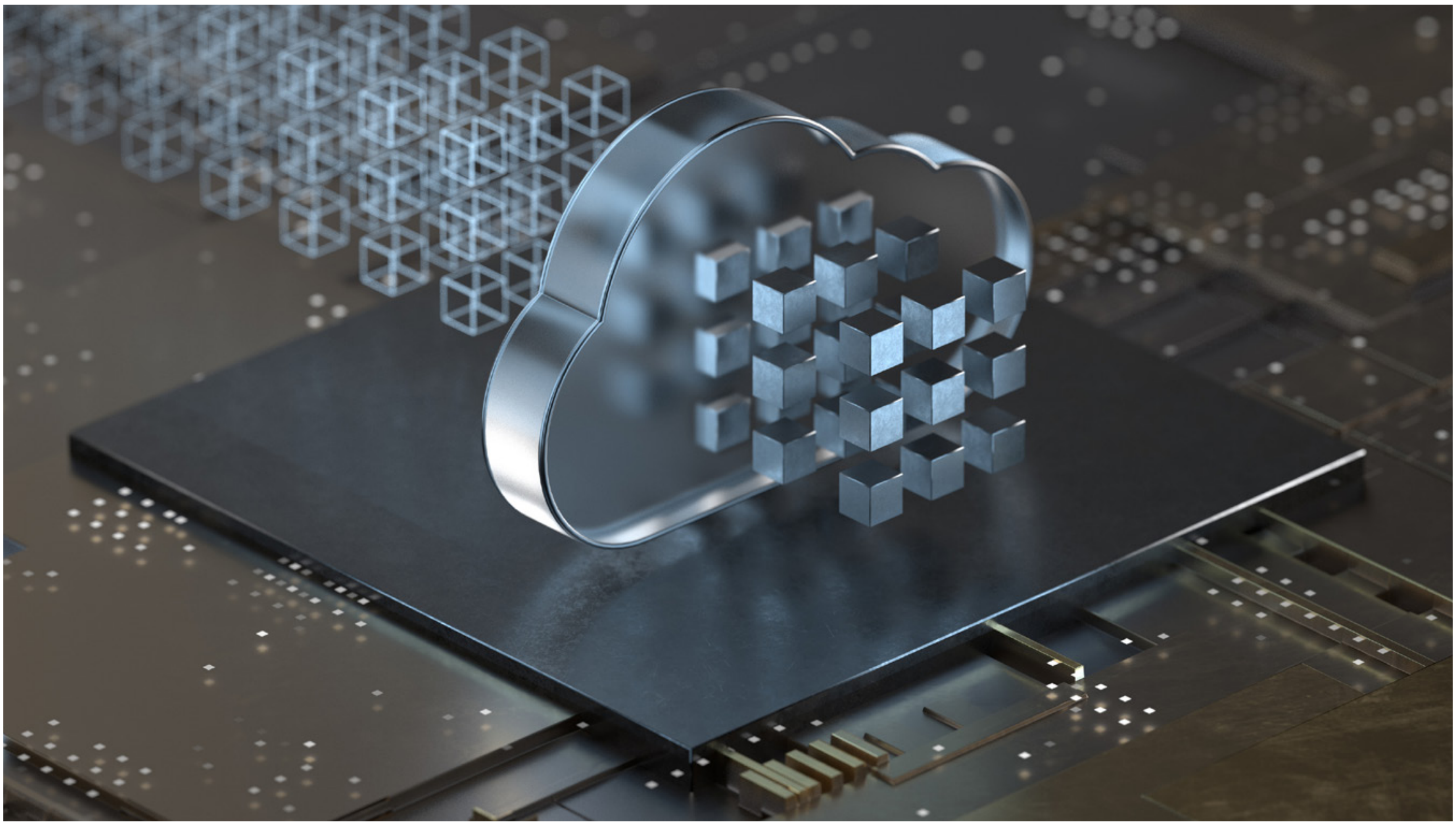
- Complete digitized product record
- Responsive change management
- Team collaboration

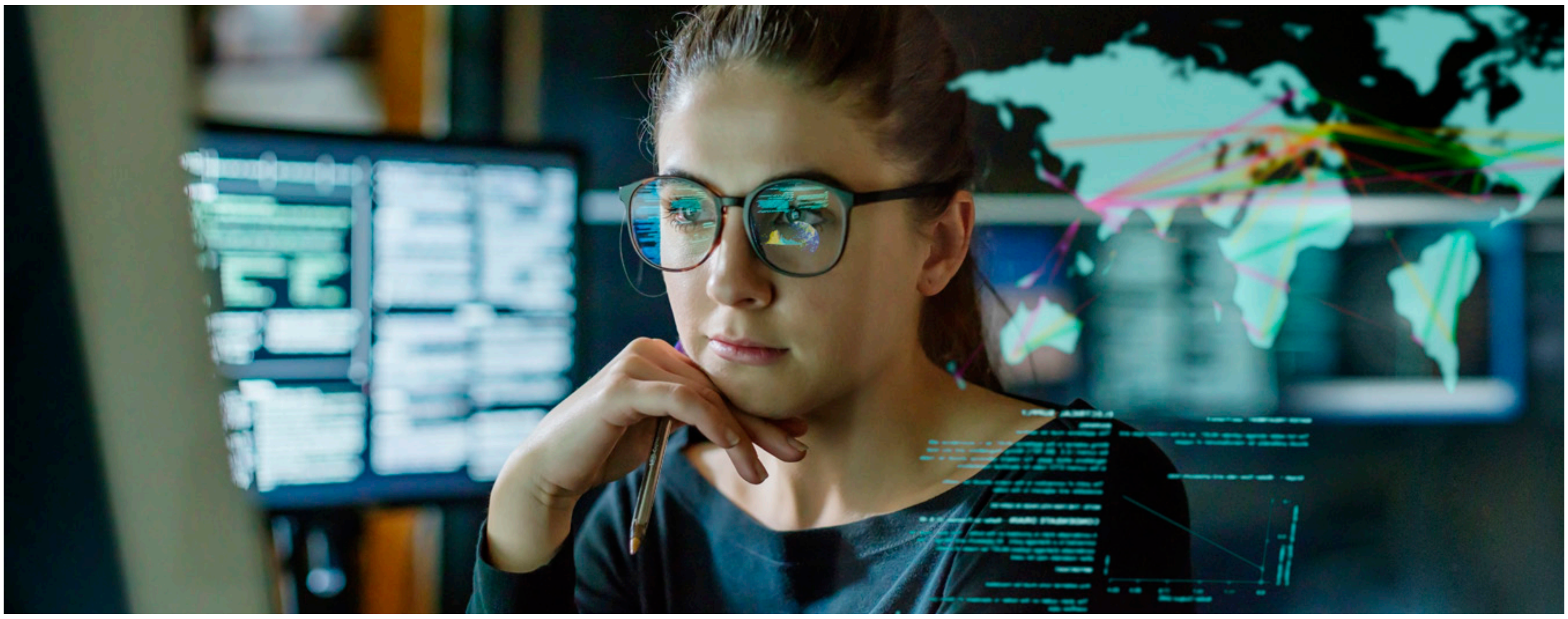
ENSURE COMPLIANCE

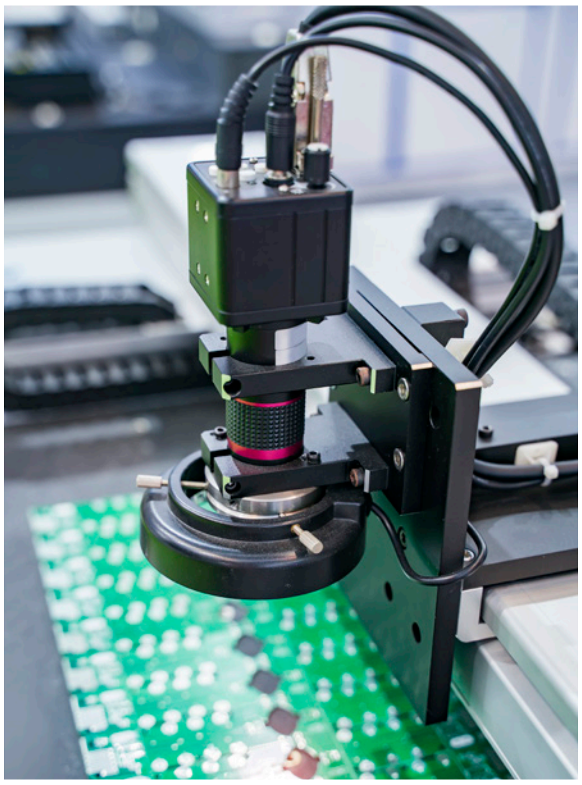
- Traceable requirements management through NPDI
- Streamlined training management
- Configured templates for process adherence

EXCEED COMMITMENTS

- Closed-loop quality processes
- Design with purpose (cost, manufacturing, serviceability)
- Product obsolescence management







HOW ARENA ACHIEVES ITAR/EAR/ CMMC COMPLIANCE AND BUSINESS OBJECTIVES

As we have noted, ITAR/EAR compliance in the Cloud focuses on ensuring that applicable technical data is not inadvertently distributed to foreign persons or foreign nations. CMMC compliance focuses on having the proper protocols, security controls, and monitoring in place to mitigate cyberattacks and safeguard sensitive information. At Arena, security and compliance are shared responsibilities between us, our data center provider, AWS GovCloud (US), and our customers (both administrators and end users).

For both defense-related and commercial product advancement, Arena PLM for AWS GovCloud provides a secure platform for unifying your entire product record. Users gain complete visibility and traceability, with support for ITAR/EAR/CMMC compliance at every phase, from requirements management to sustaining high-quality products that endure.

Arena's multilayered security model translates to significant savings of cost and time for your business since you don't have to invest in additional IT resources to build a security framework from scratch.

Purpose-Built With Proven Architecture

Arena is designed to address complex product realization and supply chain needs for companies of all sizes, from younger fast-growing companies to large global enterprises. Our multi-tenant SaaS cloud-native architecture streamlines regulatory compliance, formalizes design-control processes, and improves both communication and product quality for leading organizations.

Business-Ready by Design

Arena solves the complexities of PLM with a highly intuitive system that's easy to provision, set up, configure, and use—no coding necessary.

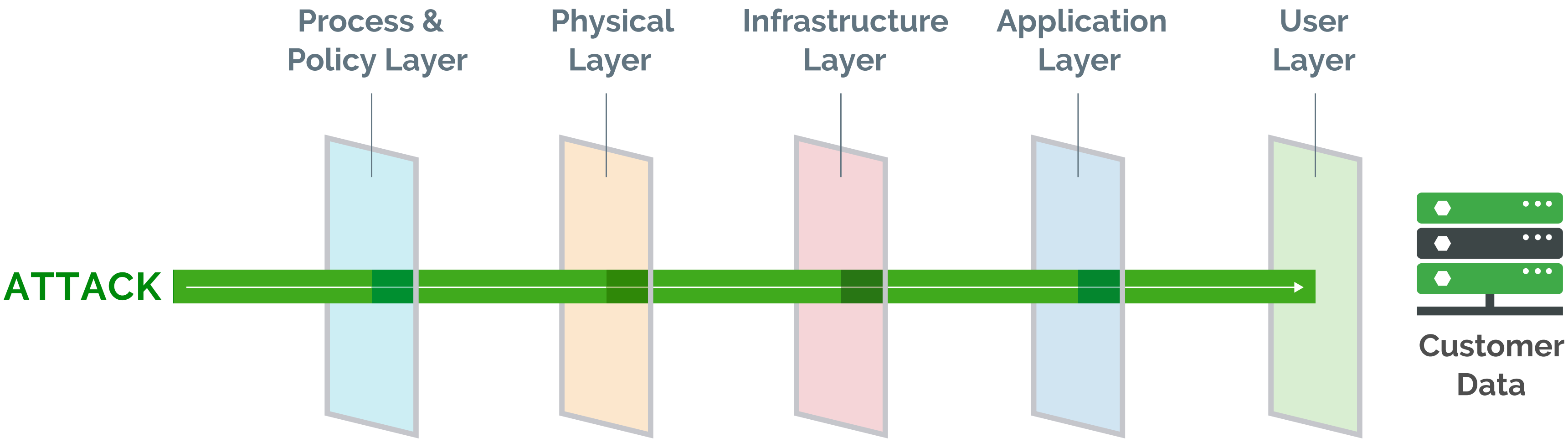
Secure AWS GovCloud Foundation

We have teamed up with best-in-class AWS GovCloud (US) to offer Arena for regulated customers. Arena's PLM for AWS GovCloud deployment is geographically located within the United States. Continuously audited by accredited third-party assessors, it supports ITAR/EAR compliance with physical and logical administrative access to U.S. citizens only and NIST SP 800-171 Standardized Reference Architecture.

Process Controls for Regulated Environments

Arena further ensures information security with firm controls on the people, tools, and processes that touch the data and systems. Secure product development in the Cloud requires attention to detail, not just in the platform foundation, but in all aspects that impact the system and data. Our approach to security process controls for the regulated environment is consistent with the requirements in NIST and DFARS. It includes employees, vulnerability assessments, internal and third-party audits, security policies and procedures, operational and security monitoring, incident response, and disaster recovery and backup.

Arena PLM Security Model



THE PATH TO SECURE PRODUCT DEVELOPMENT AND INNOVATION

ITAR/EAR/CMMC compliance no longer means organizations have to adopt manual paper-based processes or settle for limited, often expensive, on-premises PLM tools. In fact, to win defense business and maintain commercial market competitiveness, manufacturers need to embrace the power of latest technologies and tools, including cloud systems.

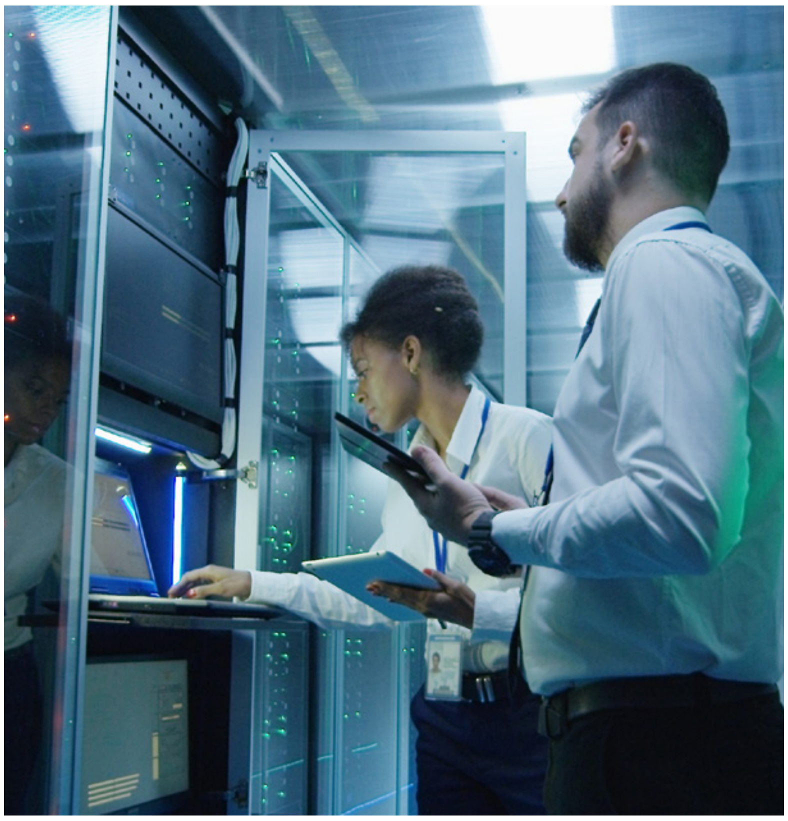
Secure, cloud-native PLM solutions provide greater flexibility, reduce overhead, and support ITAR/EAR/CMMC compliance, enabling companies to innovate faster and reach their business targets.

LEARN MORE

Meet export controls, cybersecurity, and quality management requirements: Arena PLM for AWS GovCloud

References:

1. United States Munitions List
2. Commerce Control List
3. U.S. Department of State Directorate of Defense Trade Controls
4. Bureau of Industry and Security
5. Department of Defense. Proposed Rule. 32 CFR 170. Cybersecurity Maturity Model Certification (CMMC) Program
6. Defense Outlays and Forecast in the United States from 2000 to 2033



121 Seaport Blvd, Boston, MA 02210 : ptc.com

J12599–PTC–Digital-Twin–Use–Cases–0708