A PRACTICAL FRAMEWORK

Operating AI in Aerospace Manufacturing

How US aerospace manufacturers can adopt AI under export control, CMMC and quality requirements

Edition: Q4 2026

Connect 981

Table of Contents

01 Executive summary — How to use this guide, Disclaimer and version

02 Why now — AI adoption, the aerospace risk landscape, regulatory timeline

03 The core framework — Governance, inventory, risk tiers, data classification, tools, oversight, training, monitoring

04 US regulatory requirements — ITAR/EAR, CMMC and DFARS, FAA, privacy, customer flow-downs

05 Implementation roadmap — 90-day plan and maturity self-assessment

06 Closing — What good looks like

07 Appendices
A. Model AI acceptable-use policy
B. Vendor due diligence questionnaire
C. Data classification quick reference
D. Glossary
E. Expanded self-assessment
F. Sources

Executive Summary

AI tools are already in use across aerospace manufacturing, often without a written policy. Engineers summarize specifications with chatbots, planners use AI features inside ERP systems, and quality teams test AI for inspection and root-cause analysis. The productivity gains are real. So is the exposure.

Aerospace carries risks that generic AI policies miss. Pasting export-controlled technical data into the wrong tool can be an unauthorized export. An AI tool connected to a CUI environment can put CMMC certification at risk. Customer drawings arrive with confidentiality flow-downs. And quality records must stay traceable to an accountable person.

This guide gives aerospace manufacturers a practical framework for adopting AI under those constraints. It is built on two recognized standards, the NIST AI Risk Management Framework and ISO/IEC 42001, and mapped to AS9100 so it fits the quality management system you already run.



Florent François
Chief Executive Officer



Stephanie Fels
Chief Revenue Officer

Three things every aerospace organization should do this quarter:

01

Find out what AI is already in use.

Inventory the tools, including AI features embedded in existing business systems.

02

Draw a hard line around controlled data.

Export-controlled data, CUI and customer proprietary data stay out of any AI tool that has not been explicitly approved for it.

03

Name an owner.

Give one cross-functional group the authority to approve tools, classify use cases and update the policy.

How to use this guide

This guide is written for US aerospace manufacturers and their suppliers. Part 1 explains the risks and deadlines. Part 2 sets out the core framework. Part 3 covers the US regulations that shape it: export controls, CMMC and DFARS, FAA expectations, privacy and customer flow-downs. Part 4 turns the framework into a 90-day plan. The appendices contain templates you can adapt directly.

Disclaimer and version

This guide is general information, not legal advice. Export control, defense contracting and data protection obligations depend on your specific contracts, products and jurisdictions. Confirm your obligations with qualified counsel and your export compliance officer.

Regulations covered here are changing quickly. This edition reflects the regulatory landscape as of September 2026. We plan to update it every six months.

Part 1: Why now

AI adoption in aerospace manufacturing is moving faster than the policies meant to govern it. CMMC Phase 2, which begins on November 10, 2026, makes the coming months the practical window to put AI governance in place, especially for defense suppliers.

How AI is showing up in aerospace organizations

Most AI enters aerospace organizations through three doors:

01	Public generative AI tools used by individuals:	summarizing specifications, drafting supplier emails, translating technical documents, writing code or macros.
02	AI features embedded in existing systems:	forecasting in ERP, anomaly detection in MES, search and drafting assistants in PLM and document management. These are often switched on by a vendor update, not a deliberate decision.
03	Purpose-built AI applications:	supplier risk scoring, visual inspection, predictive maintenance, production planning and operational platforms.



The first door carries the most unmanaged risk. The second is the most often overlooked. The third usually gets proper review, but not always against aerospace-specific criteria.

Open question: insert headline finding from our industry survey or customer interviews here (for example, the share of respondents with no written AI policy).

The aerospace risk landscape

Risk	What goes wrong	Who is exposed
Export control	ITAR or EAR technical data is processed on servers abroad or accessible to foreign persons, which may constitute an unauthorized export	Anyone handling defense or dual-use technical data
Controlled Unclassified Information	CUI enters a system outside the organization's assessed security boundary, undermining NIST SP 800-171 and CMMC compliance	DoD contractors and subcontractors
Customer IP and flow-downs	OEM drawings or specifications are shared with a tool whose terms allow data retention or model training, breaching confidentiality clauses	Every supplier receiving customer technical data
Quality record integrity	An AI-drafted nonconformance report, work instruction or inspection result enters the record without accountable human review	AS9100-certified organizations, repair stations, production approval holders
Personal data	Employee or partner personal data is processed without a lawful basis or adequate safeguards	Organizations subject to state privacy laws, including California's
Product safety	AI influences a decision affecting airworthiness without assurance that its outputs are reliable	Design, production and MRO organizations

---

Regulatory timeline at a glance

Date	Milestone
Nov 10, 2027	CMMC Phase 3 begins, adding Level 3 requirements for the most sensitive programs
Nov 10, 2026	CMMC Phase 2 begins: Level 2 third-party certification becomes a condition of award for contracts involving CUI
Nov 10, 2025	CMMC Phase 1 began: self-assessments required in new DoD contracts
Already in force	ITAR, EAR and DFARS 252.204-7012 apply to any AI tool that handles controlled data

Source: CMMC phased rollout.

Export control and DFARS obligations already apply to AI tools today. CMMC Phase 2 adds third-party verification, so an unassessed AI tool connected to CUI becomes a visible audit finding, not just a hidden risk.

Part 2: The core framework

The core framework applies to every organization, regardless of jurisdiction. It follows the four functions of the NIST AI Risk Management Framework (Govern, Map, Measure, Manage) and uses the management system structure of ISO/IEC 42001, which shares its clause layout with AS9100.

Framework section	NIST AI RMF function	ISO/IEC 42001	AS9100D touchpoint
2.1 Governance and accountability	Govern	Clause 5, Annex A.2–A.3	Clause 5 Leadership
2.2 AI inventory	Map	Clause 4, Annex A.6	Clause 4 Context, 7.1.6 Knowledge
2.3 Risk-tiered use cases	Map, Measure	Clause 6.1, Annex A.5	Clause 6.1 Risks, 8.1.1 Operational risk
2.4 Data classification	Manage	Annex A.7	Clause 8.5.3 Property belonging to customers or external providers
2.5 Approved tools and vendors	Manage	Annex A.10	Clause 8.4 External providers
2.6 Human oversight and records	Manage	Annex A.9	Clause 7.5 Documented information, 8.7 Nonconforming outputs
2.7 Training and AI literacy	Govern	Clause 7.2–7.3, Annex A.4	Clause 7.2 Competence, 7.3 Awareness
2.8 Monitoring and review	Measure, Manage	Clauses 9–10	Clauses 9 Evaluation, 10 Improvement

If you already run an AS9100 quality management system, you do not need a separate management system for AI. Extend the one you have.

2.1 Governance and accountability

One group owns AI decisions, with a clear escalation path. In most aerospace organizations this is an AI governance group of four to six people:

Role	Responsibility
Executive sponsor	Sets risk appetite, resolves escalations, owns the policy
Quality	Integrates AI into the QMS, owns record integrity and AS9100 alignment
Export compliance / empowered official	Rules on any use case touching ITAR or EAR data
IT and cybersecurity	Assesses tools, manages access, maintains the CUI boundary
Legal and contracts	Reviews vendor terms, customer flow-downs and privacy obligations
Operations representative	Brings real use cases and keeps the policy workable

The group approves tools, assigns risk tiers to use cases, decides exceptions and reviews the policy. Smaller organizations can combine roles, but export compliance and quality should never be absent.

2.2 AI inventory

You cannot govern what you cannot see. Build and maintain a register of every AI system in use.

For each entry, record: the tool and vendor, the business owner, the use case, the data it touches, where data is processed and stored, whether the vendor trains on your data, the risk tier and the approval date.

Three discovery methods work well together:

01	Ask.	Survey teams on what they use. Make it clear the goal is visibility, not discipline.
02	Look.	Review network and SSO logs for traffic to AI services, and expense reports for AI subscriptions.
03	Check your vendors.	Ask ERP, MES, PLM and document management vendors which AI features are active in your instance and what data they use.

2.3 Risk-tiered use cases

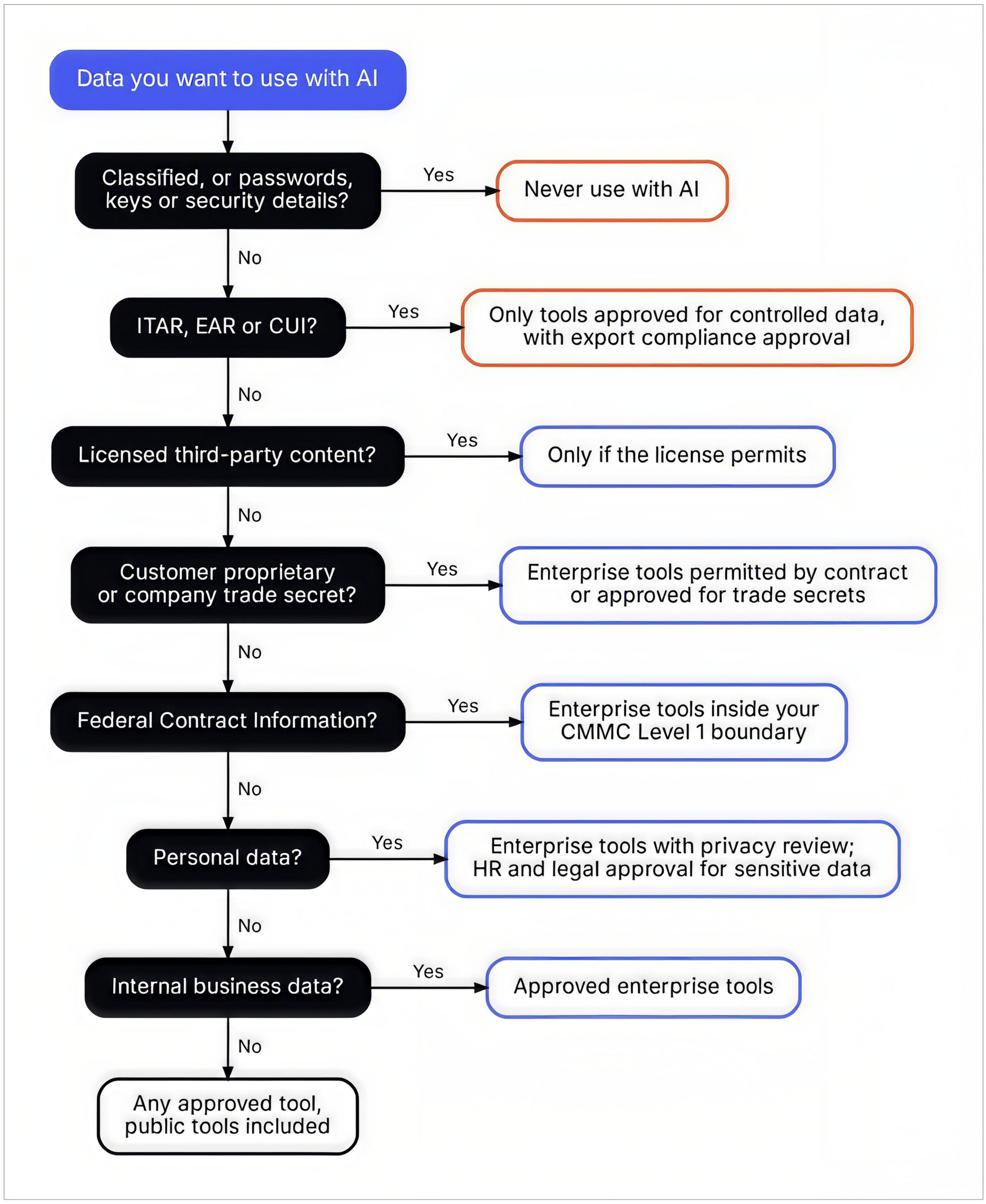
Not every AI use needs the same scrutiny. Assign every use case to one of three tiers based on the data it touches and the decisions it influences.

Tier	Definition	Aerospace examples	Required controls
Tier 1: Low	Public or internal-general data only; no effect on product, quality records or customer commitments	Drafting internal emails, summarizing public standards, brainstorming, formatting presentations	Approved tool list; acceptable-use training; no controlled data
Tier 2: Medium	Internal business data or customer data under approved terms; outputs inform decisions but a person decides	Supplier performance analysis, demand forecasting, production scheduling support, drafting supplier corrective action requests	Enterprise tool with contractual data protections; defined business owner; human review of outputs; logging
Tier 3: High	Export-controlled data, CUI, or outputs that affect product conformity, airworthiness or quality records	AI-assisted inspection, nonconformance disposition support, work instruction generation, analysis of ITAR technical data	Governance group approval; export compliance sign-off; validated performance; documented human accountability; audit trail; periodic revalidation

Some uses are prohibited outright unless the governance group grants a documented exception: entering ITAR or EAR technical data, CUI or customer proprietary data into any public AI tool, and letting AI make final dispositions on product conformity.

2.4 Data classification: can this data go into this AI tool?

Every employee should be able to answer this question in under a minute.



Data classification decision tree

When in doubt, treat data as the more restrictive category and ask export compliance. Remember that AI outputs take on the classification of their most sensitive input. Appendix C is a printable version of this decision tree.

2.5 Approved tools and vendor due diligence

Maintain a short list of approved tools, each mapped to the highest data category it may handle. The key distinction is between public consumer tools and enterprise tools with contractual protections.

Before approving any AI tool, confirm:

Data use	whether the vendor trains models on your data, and whether that can be contractually excluded.
Data location	where data is processed and stored, including subprocessors and support staff.
Access	who at the vendor can access your data, and whether foreign persons can.
Retention	how long prompts, files and outputs are kept, and whether you can delete them.
Security	certifications such as SOC 2 Type II, ISO/IEC 27001 and, for CUI, FedRAMP Moderate or equivalent.
Contract terms	confidentiality, breach notification, liability and audit rights.

Treat AI vendors as external providers under AS9100 clause 8.4. Appendix B contains a full due diligence questionnaire.

2.6 Human oversight and record integrity

AI can draft, suggest and analyze. A named person remains accountable for every output that enters a quality record, customer deliverable or product decision. For Tier 2 and Tier 3 uses:

- A qualified person reviews and approves AI-assisted content before it enters a controlled record.
- AI must not be the sole basis for accepting product, dispositioning nonconformances or signing release documentation.
- Records show that AI was used, which tool and version, and who approved the output.
- Changes to AI tools that affect Tier 3 uses go through change control, as a change to a production process would.

This aligns with AS9100 requirements for documented information and control of nonconforming outputs, and with the recordkeeping expectations of aviation authorities.

2.7 Training and AI literacy

Policy only works if people know it. Use two training tracks:

Audience	Content	Frequency
All employees	Approved tools, data classification rules, prohibited uses, how to report a concern	At onboarding and yearly
Engineers, quality, supply chain and IT staff using Tier 2–3 tools	Tool limitations and failure modes, review responsibilities, export control scenarios, record requirements	Before first use and yearly

Keep training records. They show auditors, assessors and customers that the policy is applied in practice, not just written.

2.8 Monitoring, incidents and review

Treat AI failures like quality escapes: report them, contain them and learn from them.

AI incidents	include controlled data entered into an unapproved tool, an AI output that caused or nearly caused a nonconformance, and unexpected vendor changes to data handling.
Reporting	route incidents through existing channels, the quality system for product impacts and export compliance for data exposures. Potential export violations may require a voluntary disclosure decision.
Monitoring	review Tier 3 tool performance on a set schedule and after any significant vendor update.
Review	the governance group reviews the policy, inventory and incident log at least twice a year, and includes AI in QMS management review.

Connect981 in practice. Connect981 is an AI-powered operational platform built for aerospace manufacturers, so the framework above shaped how it handles data. When you assess it as a Tier 2 or Tier 3 tool, these are the answers that matter: [where customer data is processed and stored], [who can access it and whether access can be limited to US persons], [whether customer data is used to train models], and [how AI-assisted outputs are attributed to an approving user].

Open question: product and security team to confirm each bracketed point before publishing.

Part 3: US regulatory requirements

For US aerospace organizations, export control is the most serious AI risk and CMMC is the most urgent deadline. Both turn on the same question: where your data goes and who can see it.

3.1 Export controls: ITAR and EAR

The International Traffic in Arms Regulations (ITAR) govern defense articles and technical data on the US Munitions List. The Export Administration Regulations (EAR) govern dual-use items, including much commercial aerospace technology. Both apply to technical data, not only hardware.

AI tools create export risk in three ways:

Offshore processing.	An AI service may process or store prompts and files on servers outside the US.
Foreign-person access	Vendor engineers or support staff who are foreign persons may be able to access your data. Release to a foreign person inside the US can be a deemed export
Model outputs	An AI tool fed controlled data may produce outputs that are themselves controlled technical data.

Both regulations include provisions under which sending or storing unclassified technical data is not an export, provided the data is secured with end-to-end encryption meeting specified standards and is not stored in certain prohibited countries. Most AI services cannot meet these conditions, because the service must decrypt data to process it. Do not rely on the encryption provisions for AI use without a ruling from export counsel.

Policy requirements:

01 No ITAR or EAR-controlled technical data in any AI tool unless export compliance has approved that specific tool for that data category.

02 Approved tools for controlled data must keep processing and storage in the US and restrict access to US persons, backed by contract.

03 Jurisdiction and classification determinations for data, including technology control plans, must cover AI tools.

04 Suspected exposure goes to the empowered official immediately, since voluntary disclosure decisions are time-sensitive.

3.2 Defense supply chain: CMMC, DFARS and NIST SP 800-171

DoD contractors handling Controlled Unclassified Information must protect it under DFARS 252.204-7012 and the 110 security requirements of NIST SP 800-171. CMMC adds verification. From November 10, 2026, contracting officers can require Level 2 certification by a third-party assessor as a condition of award for contracts involving CUI, and primes flow the requirement down to subcontractors.

Not all government contract data is CUI. Federal Contract Information (FCI) is non-public information provided by or generated for the government under a contract. It triggers the 15 basic safeguarding requirements of FAR 52.204-21, renumbered FAR 52.240-93 under the 2026 FAR overhaul, which CMMC Level 1 adopts. All CUI is FCI, but not all FCI is CUI. Suppliers handling only FCI still need every AI tool that touches it to sit inside their Level 1 boundary.

Any AI tool that stores, processes or transmits CUI falls inside your CMMC assessment boundary. For AI, that means:

- Cloud AI services handling CUI must meet the FedRAMP Moderate baseline or equivalent, as DFARS 7012 requires for cloud service providers.
- AI tools are listed in your System Security Plan and network diagrams if they touch CUI.
- Access controls, audit logging and incident reporting obligations extend to AI tools.
- An AI tool connected to a CUI environment without assessment can put certification at risk for the whole enclave.

The simplest policy position for most suppliers: keep AI tools outside the CUI boundary until a specific tool has been assessed and approved.

3.3 The FAA perspective

The FAA has not issued binding rules on AI in manufacturing operations. It has published a roadmap for AI safety assurance that sets out how it expects to approach AI in aviation: incremental adoption, a distinction between learned and fixed systems, and assurance proportionate to safety impact.

Two existing requirements already apply to AI use:

Production approval holders (14 CFR Part 21)	must maintain a quality system with controlled processes and records. AI that affects conformity determinations is part of that system.
Repair stations (14 CFR Part 145)	must keep accurate maintenance records and follow approved data. AI-drafted maintenance content needs the same review and sign-off as any other.

Treat any AI touching airworthiness as Tier 3 and document the human accountability chain.

3.4 Privacy

The US has no single federal privacy law for private companies. A growing number of state laws apply, and some, notably California's, cover employee and business contact data. For AI use:

- Know where employee, applicant and contact personal data sits and which AI tools touch it.
- Be cautious with AI in hiring and performance management, where several states and cities regulate automated decision-making.
- Include privacy review in vendor due diligence for any Tier 2 tool handling personal data.

3.5 Customer requirements and flow-downs

For many suppliers, the most restrictive AI rules come from customers, not regulators. Primes and OEMs impose confidentiality obligations on the technical data they share, and supplier quality requirements increasingly address data handling and AI.

- Review customer contracts, supplier quality manuals and NDAs for terms governing third-party processing and data location.
- Map each major customer's data to the tools allowed to handle it.
- When unsure whether a customer permits AI processing of their data, ask the customer in writing.

Part 4: Implementation roadmap

Most aerospace organizations can move from no policy to a working AI governance system in about 90 days, then fold it into the QMS cycle.

PHASE 1

Contain

Day 1-30

Visibility and an immediate stop to the highest-risk practices

PHASE 2

Formalize

Day 31-90

An approved policy with tools people can actually use

PHASE 3

Integrate

Ongoing

AI governance running as part of the quality system

Implementation roadmap

P-01 Contain (days 1–30)

The goal is visibility and an immediate stop to the highest-risk practices.

- [ ] Name the executive sponsor and form the governance group
- [ ] Issue interim acceptable-use rules: no ITAR, EAR, CUI or customer proprietary data in public AI tools
- [ ] Launch the AI inventory survey and log review
- [ ] Ask key software vendors which AI features are active in your systems
- [ ] Brief export compliance and quality leads on their roles

---

P-02 Formalize (days 31–90)

The goal is an approved policy with tools people can actually use.

- [ ] Adopt the AI policy, adapted from Appendix A
- [ ] Assign risk tiers to every inventoried use case
- [ ] Complete vendor due diligence for priority tools, using Appendix B
- [ ] Publish the approved tool list with the data category each tool may handle
- [ ] Distribute the data classification quick reference (Appendix C)
- [ ] Deliver all-employee training and the deeper track for Tier 2–3 users
- [ ] Review customer contracts for AI and data-processing restrictions
- [ ] Confirm with export compliance which approved tools, if any, may handle ITAR, EAR or CUI data

---

P-03 Integrate (ongoing)

The goal is AI governance that runs as part of the quality system.

- [ ] Add AI controls to the internal audit program
- [ ] Include AI in QMS management review
- [ ] Revalidate Tier 3 tools on a fixed schedule and after major vendor updates
- [ ] Review the policy twice a year against regulatory changes
- [ ] Track CMMC phase dates and new federal and state AI requirements

AI governance maturity self-assessment

Score each statement: 0 = not in place, 1 = partly in place, 2 = fully in place.

#	Statement	Score (0-2)
01	A named group owns AI decisions, including quality and export compliance	
02	We have a current inventory of AI tools, including embedded features	
03	Every AI use case has an assigned risk tier	
04	Employees know which data may go into which tools	
05	Public AI tools are blocked from export-controlled data and CUI in practice, not just on paper	
06	We have reviewed the data terms of every approved AI vendor	
07	AI-assisted quality records show the tool used and the approving person	
08	We know which customer contracts restrict AI processing	
09	Staff using AI have received role-appropriate training	
10	AI incidents have a defined reporting route	
11	AI is covered by internal audit and management review	
12	Every AI tool that touches CUI is inside our assessed CMMC boundary, or blocked from it	

Total score	Maturity level	Meaning
0-8	Exposed	AI is in use without meaningful control; start with Phase 1 now
9-16	Developing	Foundations exist, but gaps remain in controlled data or records
17-24	Governed	AI governance is operating; focus on integration and revalidation

This 12-question version gives a quick read. For a full assessment, use the expanded version in Appendix E.

Connect981 in practice. Phase 2 is where most teams stall: vendor due diligence and approved tools take longer than expected. For Connect981, we provide [our completed vendor questionnaire answers, mapped to Appendix B] and [security documentation and certifications] up front, so it can move through your review without delaying the rest of the roadmap.

Open question: confirm which documents we can share and under what terms.

Closing: What good looks like

In a well-governed aerospace organization, AI is useful precisely because its boundaries are clear. People use it confidently, because they know what they can and cannot do.

A supply chain analyst uses an approved enterprise tool to review six months of supplier delivery and quality data and flags three suppliers trending toward escapes. She knows the data is within the tool's approved category. She makes the call on which suppliers to escalate, and the analysis is saved with the corrective action request.

An engineer needs to compare two revisions of an ITAR-controlled specification. He does not paste it into a public chatbot. He uses the one tool export compliance has approved for that data, which runs inside the company's controlled environment.

A quality manager preparing for an AS9100 surveillance audit shows the auditor the AI inventory, the risk tiers, the training records and the review log. AI is one more controlled process in the QMS, not a separate problem.

How Connect981 approaches this

Connect981 is an AI-powered operational platform built for aerospace manufacturers in commercial and defense programs. We designed it around the constraints described in this guide: controlled data, customer confidentiality, traceable decisions and human accountability.

Open question: add two or three verified specifics on how Connect981 handles data location, access controls and customer data use, confirmed by the product and security team before publishing.

To discuss how these principles apply to your operations, contact us at connect981.com.



Appendix A: Model AI acceptable-use policy

Adapt this template to your organization. Bracketed text marks the choices you need to make.

[Company] Artificial Intelligence Acceptable-Use Policy

Version [x.x] · Effective [date] · Owner: [AI governance group]

01 Purpose

This policy sets the rules for using AI tools at [Company] so that we gain their benefits while protecting controlled data, customer information, product quality, intellectual property and personal data.

02 Scope

This policy applies to all employees, contractors and temporary staff, and to all AI tools, including:

- generative AI tools such as chatbots and writing, coding and image assistants
- AI features within other software, such as ERP, MES, PLM and office suites
- AI agents: tools that take actions in other systems, such as updating records, sending messages or running code

03 Accounts and approved tools

- Only tools on the Approved AI Tool List may be used for [Company] work. Each tool is approved for specific data categories. Using a tool with data above its approved category is prohibited.
- Use only [Company]-provided accounts for work. Personal AI accounts, free tiers and browser extensions must not be used with [Company] or customer data.

04 Prohibited uses

Unless the AI governance group has granted a written exception, you must not:

- enter ITAR or EAR-controlled technical data, CUI or customer proprietary data into any tool not approved for it
- enter any of the above into public AI tools under any circumstances
- use AI output as the sole basis for accepting product, dispositioning nonconformances or signing release documentation
- use AI to make employment decisions about individuals without HR and legal review
- use AI to reproduce third-party copyrighted material, trademarks or confidential information belonging to others

05 Your responsibilities

- Classify data before using it with AI; when unsure, ask [export compliance contact]
- Review AI output for accuracy, completeness and bias before relying on it; you are accountable for anything you use, send or sign
- Have AI-generated code, scripts and macros reviewed for errors and security vulnerabilities before they run in production systems
- Disclose AI use when sharing work with customers or regulators, and record it in controlled records as required by [QMS procedure reference]
- Report suspected misuse or data exposure immediately to [contact]

06	AI agents and automated actions	• AI agents may act only within the permissions approved for them, using dedicated service accounts, never your personal credentials • Actions that change controlled records, send external communications or affect production require human approval before they take effect • Agents must not be connected to systems holding ITAR, EAR or CUI data unless approved for that data category
07	Data retention and logging	• Approved tools are configured so [Company] data is not used to train vendor models • Prompts, files and outputs are retained only as long as [retention period] and deleted in line with [records retention policy] • Use of Tier 2 and Tier 3 tools is logged and logs are kept for [period] to support audits, investigations and CMMC assessment evidence
08	Requesting new tools or use cases	Submit requests through [request form or ticket queue]. Include the tool, the use case and the data involved. The AI governance group assigns a risk tier and required controls, and responds within [target time]. Do not use a tool while it is under review.
09	Training	Complete AI training at onboarding and yearly. Tier 2 and Tier 3 tool users complete additional training before first use.
10	Acknowledgement	All staff in scope confirm in writing that they have read and will follow this policy, at onboarding and after each material revision.
11	Violations	Violations are handled under [disciplinary policy]. Potential export control violations are referred to [empowered official].
12	Review	The AI governance group reviews this policy at least twice a year, and after any significant AI incident, regulatory change or new category of AI tool.

Appendix B:
AI vendor due diligence questionnaire

Use this questionnaire to screen AI vendors before approval. For Tier 3 tools, also ask for deeper evidence such as a completed CSA AI-CAIQ self-assessment or an equivalent third-party assessment.

Area	Question	Acceptable answer for controlled data
Data use	Do you use customer inputs or outputs to train or improve models?	No, contractually guaranteed
Data use	Can training use be disabled at the account level?	Yes, and it is off by default
Location	In which countries are data processed and stored, including backups?	US only for ITAR/CUI; approved jurisdictions otherwise
Location	Which subprocessors handle our data, and where?	Full list provided, same location limits
Fourth-party AI	Which foundation models and AI providers power your service, and on what data terms?	Named providers; no-training, location and access terms flow down to them
Access	Who at your company can access our data, and under what conditions?	Named roles, logged, on request only
Access	Can you restrict access to US persons or specific nationalities?	Yes, contractually and technically
Retention	How long do you keep prompts, files and outputs?	Configurable; zero retention available
Retention	Can we delete our data on request and receive confirmation?	Yes, within a defined period
Security	Which certifications do you hold?	SOC 2 Type II, ISO/IEC 27001; FedRAMP Moderate or equivalent for CUI
Security	How do you test for prompt injection, data leakage between customers and other AI-specific attacks?	Regular red-teaming and third-party testing; summary available on request
Security	How quickly do you notify customers of security incidents?	Fast enough for us to meet the DFARS 72-hour reporting deadline for CUI incidents, set in the contract
Integration	What access to our systems does the tool need, and do you support SSO, MFA and role-based permissions?	Least-privilege access; SSO and MFA supported; granular roles
Integration	Are administrator and AI agent actions logged, and can we export the logs?	Yes, with logs exportable to our security monitoring
Model lifecycle	How do you test new models before release, and how do you notify customers of changes that could affect outputs?	Documented evaluation; advance notice with version history

Area	Question	Acceptable answer for controlled data
Model lifecycle	Can we stay on a specific model version for critical uses?	Yes, for a defined period
AI governance	Do you follow NIST AI RMF, hold ISO/IEC 42001 certification, or publish a CSA AI-CAIQ self-assessment?	Yes, or a documented equivalent
Outputs and IP	Who owns the outputs, and do you indemnify us against third-party IP claims arising from them?	We own outputs; vendor provides IP indemnity
Privacy	Will you sign a data processing agreement meeting applicable privacy laws?	Yes
Contract	Do you accept confidentiality terms matching our customer flow-downs?	Yes
Exit	Can we export our data and configurations, and what happens to our data at contract end?	Full export in a usable format; certified deletion within a defined period
Continuity	What availability do you commit to, and what is your continuity plan if the service fails?	Contractual SLA; documented and tested continuity plan

How to read the answers:

Disqualifying for Tier 3:

any answer short of the acceptable one on training use, data location, US-person access or fourth-party terms. The tool may still be approved for lower tiers.

Fixable through contract:

gaps on retention, incident notification, IP indemnity or exit terms can often be closed in negotiation. Approve only once the contract reflects them.

Record the outcome:

file the completed questionnaire, the tier decision and any conditions in the AI inventory, and repeat the review yearly or after a major vendor change.

Appendix C: Data classification quick reference

Data category	Examples	Public AI tools	Approved enterprise AI tools	Tools approved for controlled data
Classified	Any classified national security information	Never	Never	Never; outside the scope of this guide
Credentials and security information	Passwords, API keys, private keys, network diagrams of CUI systems	Never	Never	Never
Export-controlled / CUI	ITAR drawings, EAR technical data, CUI	Never	Never	Only with export compliance approval

Data category	Examples	Public AI tools	Approved enterprise AI tools	Tools approved for controlled data
Licensed third-party content	Purchased industry standards, licensed datasets and documentation	Never	Only if the license permits	Only if the license permits
Customer proprietary	OEM specifications, drawings under NDA	Never	Only if the customer contract permits	Yes, if the contract permits
Company trade secrets	Manufacturing processes, proprietary designs, cost models, pricing	Never	Only tools approved for trade secrets, with no vendor training	Yes
Federal Contract Information (FCI)	Non-public government contract information, such as delivery schedules, quantities and statements of work	Never	Only tools inside your CMMC Level 1 boundary	Yes
Sensitive personal data	Social Security numbers, health information, background-check results	Never	Only with HR, legal and privacy approval	Only with HR, legal and privacy approval
Personal data	Employee contact details, training records, contact lists	Never	With privacy review	With privacy review
Internal business	Internal schedules, supplier performance, operating metrics	No	Yes	Yes
Public / internal-general	Published standards summaries, marketing content, generic questions	Yes	Yes	Yes

Three rules apply to every category:

AI outputs take on the highest classification of their inputs

A summary of an ITAR drawing is still ITAR data, and must be stored and shared as such.

Combining data can raise its classification

Several individually harmless datasets can become sensitive together, such as supplier lists combined with program schedules. Classify the combination, not just the parts.

Unmarked does not mean uncontrolled

Export control and CUI status depend on what the data is, not on whether it carries a label.

When in doubt, use the more restrictive category and ask export compliance.

Appendix D: Glossary

Term	Meaning	See
AI agent	An AI tool that takes actions in other systems, such as updating records, sending messages or running code, rather than only producing text	App. A
AI inventory	The register of every AI tool and AI feature in use, with its owner, data, risk tier and approval status	2.2
AS9100	Quality management system standard for aviation, space and defense organizations	Part 2
C3PAO	CMMC Third-Party Assessment Organization, authorized to certify contractors at Level 2	3.2
CMMC	Cybersecurity Maturity Model Certification, the DoD program verifying contractor cybersecurity	3.2
CMMC assessment boundary	The systems, people and facilities that store, process or transmit FCI or CUI, and so fall within scope of a CMMC assessment	3.2
CSA AI-CAIQ	Cloud Security Alliance questionnaire, mapped to its AI Controls Matrix, that AI vendors use to self-assess their security and governance controls	App. B
CUI	Controlled Unclassified Information: government information requiring safeguarding but not classified	3.2
Deemed export	Release of controlled technology to a foreign person inside the country, treated as an export to that person’s country	3.1
DFARS	Defense Federal Acquisition Regulation Supplement, including clause 252.204-7012 on safeguarding CUI	3.2
EAR	Export Administration Regulations, the US regime for dual-use items	3.1
Empowered official	The person an organization designates under ITAR with authority to sign export license applications and to stop transactions that may breach export rules	3.1
FAR	Federal Acquisition Regulation, the government-wide rules for federal procurement; DFARS supplements it for defense contracts	3.2
FCI	Federal Contract Information: non-public information provided by or generated for the government under a contract, protected under FAR 52.204-21 (now 52.240-93) and CMMC Level 1	3.2
FedRAMP	US government program for authorizing cloud services	3.2
Flow-down	A contract requirement a customer passes on to its suppliers, such as confidentiality, cybersecurity or export obligations	3.5
Foundation model	A large, general-purpose AI model, often built by a third party, on which many AI products are based	App. B

Term	Meaning	See
Fourth-party AI	An AI provider used by your vendor rather than by you directly; your data reaches it through the vendor	App. B
Generative AI	AI that produces new content, such as text, code or images, in response to prompts	Part 1
ISO/IEC 27001	International standard for information security management systems	App. B
ISO/IEC 42001	International standard for AI management systems	Part 2
ITAR	International Traffic in Arms Regulations, the US regime for defense articles and technical data	3.1
Large language model	A type of generative AI trained on large amounts of text to understand and produce language	Part 1
Model training on customer data	A vendor practice of using customers' prompts, files or outputs to improve its AI models, which can expose that data beyond the customer	App. B
NIST AI 600-1	NIST's Generative AI Profile, applying the AI RMF to the specific risks of generative AI	App. F
NIST AI RMF	NIST Artificial Intelligence Risk Management Framework	Part 2
NIST SP 800-171	NIST standard setting 110 security requirements for protecting CUI	3.2
Nonconformance	A product or process that does not meet a specified requirement, recorded and dispositioned under the quality system	2.6
Production approval holder	An organization holding an FAA production approval under 14 CFR Part 21 to manufacture aviation products or parts	3.3
Prompt injection	An attack in which hidden instructions in a document, web page or message manipulate an AI tool into ignoring its rules or leaking data	App. B
Red-teaming	Structured testing in which experts try to make an AI system fail or misbehave, to find weaknesses before attackers do	App. B
Repair station	A maintenance organization certificated by the FAA under 14 CFR Part 145	3.3
Risk tier	This guide's three-level classification of AI use cases (Tier 1 low, Tier 2 medium, Tier 3 high), which sets the controls each use requires	2.3
SOC 2 Type II	An independent audit report on a service provider's security controls over a period of time	App. B
System Security Plan (SSP)	The document describing a contractor's CUI environment and how it meets NIST SP 800-171; AI tools touching CUI must be included	3.2
Technical data	Information needed to design, produce, operate, repair or modify controlled items, such as drawings, specifications and work instructions; controlled under ITAR and EAR	3.1
Technology control plan	An organization's documented measures to prevent unauthorized access to export-controlled technology	3.1
US person	A US citizen, lawful permanent resident, protected individual or US-incorporated entity. Anyone else is a foreign person	3.1

Appendix E: Expanded AI governance self-assessment

This assessment covers the full framework in 32 statements, grouped by the sections of Part 2 plus customer and regulatory obligations. Use it for a baseline before Phase 1 and again at the end of Phase 2. How to score:

01

Score each statement 0 (not in place), 1 (partly in place) or 2 (fully in place, with evidence you could show an auditor).

02

Multiply the score by the weight. Weight ×2 marks the controls that matter most for export control, CMMC and product integrity.

03

Add the weighted scores. The maximum is 82.

#	Area	Statement	Weight	Score (0-2)	Weighted
01	Data	Employees can tell which data may go into which tools, using a quick reference such as Appendix C	x1		
02	Data	Public AI tools are technically blocked from ITAR, EAR and CUI data, not just prohibited on paper	x2		
03	Data	Every AI tool that touches FCI or CUI is inside our assessed CMMC boundary, or blocked from it	x2		
04	Data	Our rules treat AI outputs as carrying the classification of their most sensitive input	x1		
05	Governance	An executive sponsor is named and owns the AI policy	x1		
06	Governance	The AI governance group includes quality, export compliance, IT security and legal	x2		
07	Governance	A written AI policy is approved and published to all staff	x1		
08	Governance	Exceptions to the policy are documented and approved by the governance group	x1		
09	Risk tiers	Every AI use case has an assigned risk tier	x1		
10	Risk tiers	Every Tier 3 use has governance group approval and export compliance sign-off	x2		
11	Risk tiers	Prohibited uses are defined and communicated to staff	x1		
12	Tools and vendors	We publish an approved tool list showing the data category each tool may handle	x1		

#	Area	Statement	Weight	Score (0-2)	Weighted
13	Tools and vendors	Every approved AI vendor has completed our due diligence questionnaire	x1		
14	Tools and vendors	Vendor contracts prohibit training models on our data	x2		
15	Tools and vendors	We know which foundation models and AI providers our vendors rely on	x1		
16	Tools and vendors	Staff use company accounts for AI tools, and personal accounts are prohibited	x1		
17	Oversight and records	AI-assisted quality records show the tool used and the approving person	x2		
18	Oversight and records	AI is never the sole basis for accepting product, dispositioning nonconformances or signing release documentation	x2		
19	Oversight and records	Changes to Tier 3 AI tools go through change control	x1		
20	Oversight and records	AI agents act only within approved permissions, with human approval before changing controlled records	x1		
21	Oversight and records	AI-generated code and scripts are reviewed before they run in production systems	x1		
22	Inventory	We have a current inventory of AI tools, including AI features embedded in existing systems	x2		
23	Inventory	Each inventory entry records the owner, data used, processing location, vendor training use and risk tier	x1		
24	Inventory	The inventory is kept current through vendor checks and log reviews, not only staff surveys	x1		
25	Training	All staff have completed AI training and acknowledged the policy in writing	x1		
26	Training	Tier 2 and Tier 3 tool users have completed role-specific training	x1		
27	Monitoring	AI incidents are defined and have a clear reporting route	x1		
28	Monitoring	Suspected export-controlled data exposure goes straight to the empowered official	x2		
29	Monitoring	Tier 3 tools are revalidated on a schedule and after major vendor updates	x1		

#	Area	Statement	Weight	Score (0-2)	Weighted
30	Monitoring	AI is covered by internal audit and QMS management review	x1		
31	Customers & regulation	We know which customer contracts restrict AI processing of their data	x1		
32	Customers & regulation	We track CMMC deadlines and AI-related requirements in new contracts	x1		

Weighted total	Maturity level	Meaning
0–27	Exposed	AI is in use without meaningful control; start Phase 1 now
28–55	Developing	Foundations exist, but gaps remain in controlled data, vendors or records
56–82	Governed	AI governance is operating; focus on integration and revalidation

One override applies: if any ×2 statement scores 0, the overall level cannot be higher than Developing, whatever the total. Those gaps carry export, CMMC or product risk that a high score elsewhere does not offset.

Appendix F: Sources and further reading

Sources consulted for this edition:

- CMMC Phase 2 timeline
- CMMC Phase 2 preparation (Secureframe)
- Future of Privacy Forum: Generative AI for Organizational Use, Internal Policy Considerations
- NSA, CISA, FBI and partners: AI Data Security, Best Practices for Securing Data Used to Train and Operate AI Systems (May 2025)
- Cloud Security Alliance: AI Controls Matrix and AI-CAIQ
- FS-ISAC: Generative AI Vendor Risk Assessment Guide

Primary sources to cite directly in the published edition:

- NIST AI Risk Management Framework (AI RMF 1.0) and Generative AI Profile (NIST AI 600-1)
- ISO/IEC 42001:2023, Artificial intelligence management system
- ITAR (22 CFR Parts 120–130) and EAR (15 CFR Parts 730–774)
- 32 CFR Part 170 (CMMC Program) and DFARS 252.204-7012
- NIST SP 800-171
- FAA Roadmap for Artificial Intelligence Safety Assurance
- State privacy laws, including the California Consumer Privacy Act as amended

Connect 981

Aerospace manufacturing, made intelligent.

Let’s Connect.
Let’s Move Forward.

+1 917-499-9365
stephanie@connect981.com
connect981.com