WORKING PAPER · MARCH 2026

Authorization Readiness Levels™

A Framework for Dual-Use Companies Navigating the Pathway to Authority to Operate

Ryan Gutwein

Extending MIT's Dual-Use Readiness Levels™ for ATO Strategy

Introduction

MIT's Dual-Use Readiness Levels™ framework gave the defense tech ecosystem a shared language for measuring startup maturity across five dimensions: technology, commercial funding, commercial customers, mission funding, and mission customers. It was a breakthrough in helping founders, investors, and government stakeholders understand where a dual-use company stands — and what it needs to do next.

But the framework has a critical gap.

For any software company selling into the Department of Defense (DoD) or broader public sector, there is a sixth dimension that often determines whether a promising product ever reaches the warfighter: **authorization to operate**. Whether you are pursuing FedRAMP, navigating the DoD Risk Management Framework (RMF) through eMASS, targeting Impact Level 4 or 5 Provisional Authorization through DISA, building toward a Continuous Authority to Operate (cATO) through DevSecOps, or achieving CMMC certification to protect Controlled Unclassified Information across the defense industrial base, the ATO journey is its own multi-year, multi-stakeholder undertaking — with its own readiness levels.

This document introduces **Authorization Readiness Levels (ARL)** — a complementary framework that maps the pathway from “we know we need an ATO” to “we hold production authorizations across multiple agencies and pathways.”

The framework covers five distinct authorization pathways, each with a 9-level progression:

1. **FedRAMP Authorization Readiness Level (FARL)** — The federal civilian baseline under the unified authorization model with Rev 5 and emerging FedRAMP 20x pathway
2. **DoD RMF Authorization Readiness Level (RARL)** — The DoD Risk Management Framework pathway through eMASS, governed by NIST 800-53 and DISA STIGs
3. **Impact Level Authorization Readiness Level (IARL)** — The CC SRG pathway to IL4, IL5, and IL6 Provisional Authorizations, managed by DISA
4. **Continuous ATO Readiness Level (CARL)** — The DevSecOps-native pathway aligned with the DoD Enterprise DevSecOps Reference Design and SWFT
5. **CMMC Readiness Level (CMRL)** — The Cybersecurity Maturity Model Certification pathway, governed by 32 CFR and DFARS 252.204-7021

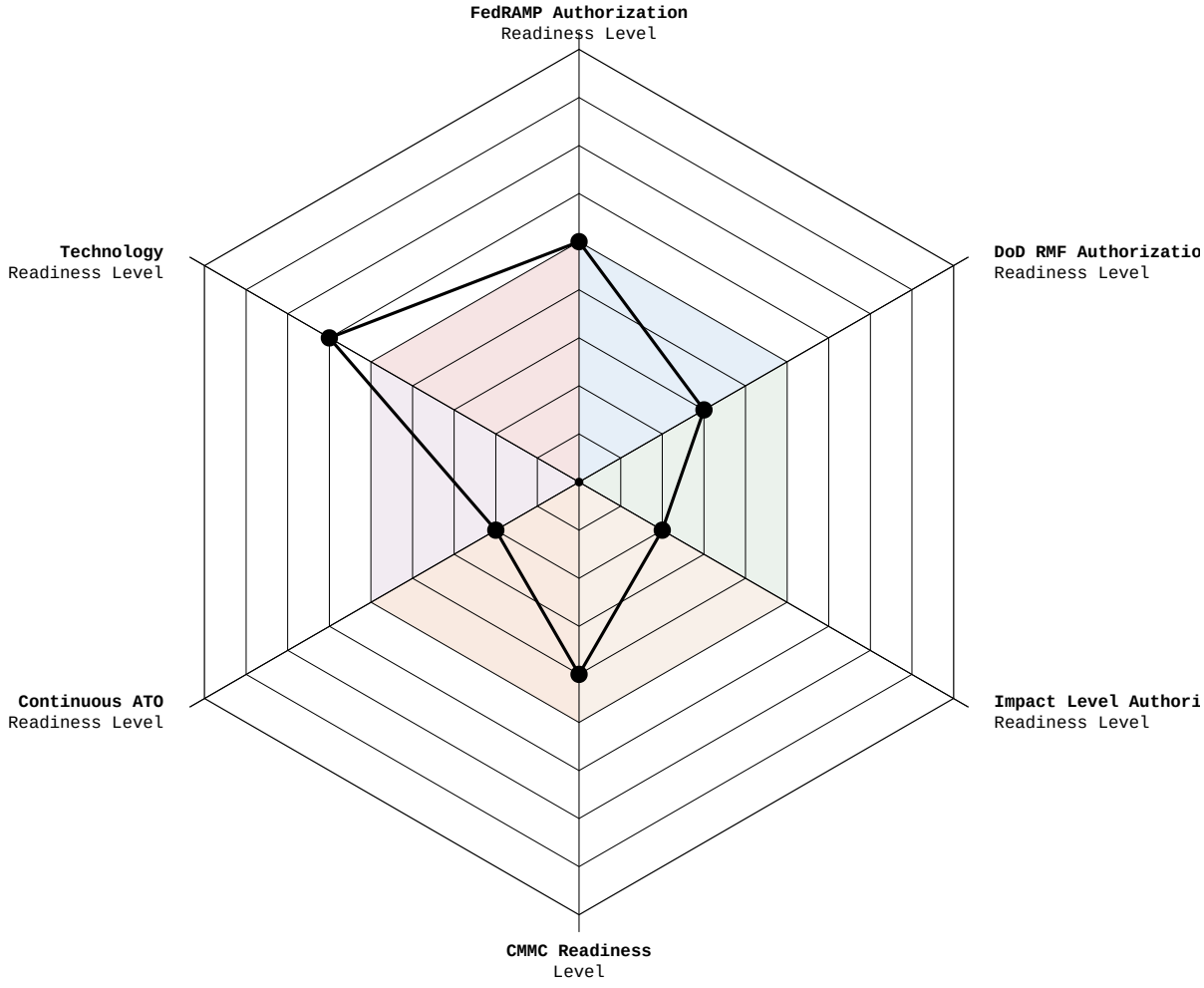

Image 1 — The Authorization Readiness Level Diagram for startup self-assessment

Image 1 — *Plot your company's current level on each axis to identify gaps and prioritize investment.*

Why Authorization Readiness Matters for Dual-Use Strategy

For commercial software companies entering the defense and public sector markets, the ATO is often the single longest pole in the tent. A company can achieve MCRL 6 (letters of intent from mission stakeholders) and MFRL 5 (procurement relationships with mission partners) on MIT's framework, yet remain completely blocked from deployment because their system lacks authorization.

The authorization journey intersects with every other readiness dimension:

- **Technology Readiness (TRL):** Your architecture decisions at TRL 3–5 will determine whether your system is authorizable at all.
- **Mission Funding (MFRL):** SBIR Phase II and III awards increasingly expect authorization pathway plans. OTA agreements often include ATO milestones as deliverables.
- **Mission Customer (MCRL):** An Authorizing Official (AO) must sign your ATO. That AO is a mission customer stakeholder.
- **Commercial Customer (CCRL):** FedRAMP authorization is increasingly valued by commercial enterprise customers as a trust signal.
- **Commercial Funding (CFRL):** Investors increasingly evaluate ATO readiness as a proxy for government revenue predictability.

How to Use This Framework

Like MIT's Dual-Use Readiness Levels, Authorization Readiness Levels are designed for **self-assessment**. Founders, CISOs, compliance leads, and government affairs teams should use this framework to:

1. **Identify where you are** across each authorization pathway you are pursuing
2. **Identify what is blocking you** from advancing to the next level
3. **Align internal teams** around a shared understanding of authorization maturity
4. **Communicate with investors and government stakeholders** using a common vocabulary
5. **Sequence your ATO strategy** — most dual-use companies should not pursue all five pathways simultaneously

Pathway Selection Guidance

- **Start with FedRAMP** if your product serves federal civilian agencies or if you need the broadest reuse potential across government.
- **Start with DoD RMF** if you have a specific DoD program sponsor and a defined system boundary within a DoD enclave.

- **Pursue IL4/IL5 PA through DISA** when you need to process CUI or National Security Systems data in a DoD cloud environment.
- **Pursue cATO** when you have a mature DevSecOps pipeline and a DoD program office willing to sponsor continuous monitoring.
- **Pursue CMMC** if you handle FCI or CUI as a defense contractor. CMMC certification is becoming a prerequisite for contract award.

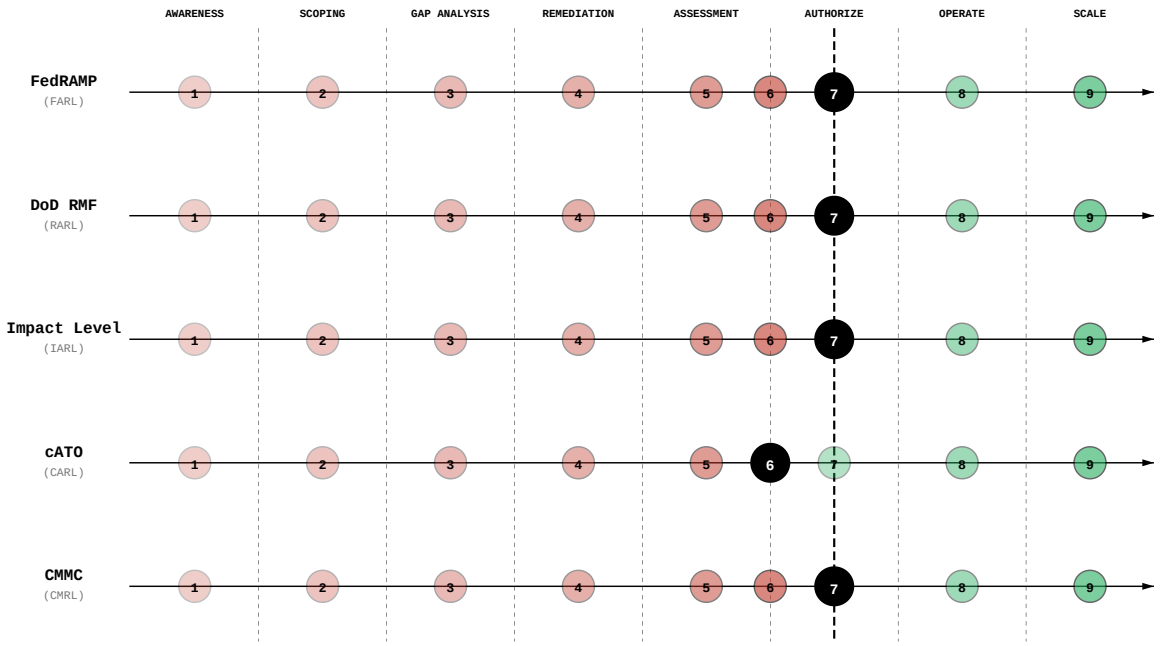

Image 2 — Five Pathways to Authority to Operate (Levels 1–9)

Image 2 — *Five ATO pathways in parallel. The black milestone circle marks the authorization inflection point.*

FedRAMP Authorization Readiness Level (FARL)

The FedRAMP Authorization Readiness Level assesses a dual-use company's progress in achieving and maintaining a FedRAMP Authorization. Following the dissolution of the Joint Authorization Board (JAB) in August 2024 and the transition to a single unified "FedRAMP Authorized" designation, all CSPs now follow one of three emerging paths: Agency Authorization (sponsored by a federal agency), Program Authorization (issued by the FedRAMP Director for widely-used services without agency sponsors), or the new FedRAMP 20x pathway (automation-driven, sponsorless continuous validation). The FedRAMP PMO, housed at GSA, manages the program, while the new FedRAMP Board (replacing the JAB) sets strategy and policy.

1 Awareness and Initial Assessment

The company recognizes that FedRAMP authorization is necessary for its federal go-to-market strategy and has begun initial research.

At this level, the company is learning the basics of FedRAMP: the unified authorization model, the meaning of Low/Moderate/High baselines, the difference between Agency Authorization, Program Authorization, and the 20x pathway, and the general scope of effort required. Leadership understands that FedRAMP is not a checkbox but a sustained operational commitment.

> **Example:** A cybersecurity analytics startup has won its first federal pilot through an OTA and realizes that production deployment will require FedRAMP Moderate authorization. The CTO begins researching FedRAMP requirements, attends Community Working Group sessions hosted by the FedRAMP PMO, and evaluates whether the traditional Rev 5 path or the emerging 20x pathway is the better fit for their cloud-native architecture.

2 Architecture and Boundary Scoping

The company has defined its system boundary, identified its cloud service model (IaaS/PaaS/SaaS), and begun mapping its architecture to FedRAMP requirements.

The company has drafted an initial SSP outline, identified whether it will leverage an existing FedRAMP-authorized IaaS/PaaS provider (inheritance model), and begun scoping the control baseline. Key architectural decisions are being made with authorizability in mind. For companies pursuing FedRAMP 20x, this phase also

includes evaluating whether existing tooling can produce the machine-readable Key Security Indicators (KSIs) that the 20x pathway requires.

> **Example:** The startup selects AWS GovCloud as its infrastructure provider, enabling inheritance of approximately 60% of NIST 800-53 Moderate controls. The team creates initial data flow diagrams and begins identifying which controls are fully inherited, shared, or customer-responsible. They also assess their observability stack for compatibility with FedRAMP 20x KSI requirements.

3 Readiness Assessment and Gap Analysis

The company has engaged a FedRAMP 3PAO or qualified consultant for a readiness assessment and has a documented gap analysis.

A formal readiness assessment has been conducted, producing a Readiness Assessment Report (RAR) or equivalent gap analysis. The company understands exactly which controls are not yet implemented, which policies need to be written, and what technical remediation is required. Note: under the evolving FedRAMP 20x model, the 3PAO role is shifting from reviewing narrative documentation to independently verifying machine-readable compliance evidence and KSIs. Under the Rev 5 program certification (sponsorless) path proposed in RFC-0023, the FedRAMP Ready designation is being phased out — new submissions will no longer be accepted after July 2026.

> **Example:** The startup engages a FedRAMP 3PAO to conduct a readiness assessment. The 3PAO identifies 47 control gaps, primarily in continuous monitoring (CA family), incident response (IR family), and configuration management (CM family). The company builds a remediation roadmap with estimated timelines and resource requirements.

4 Remediation and Documentation In Progress

The company is actively remediating control gaps and developing the full FedRAMP documentation package.

This is the heavy-lift phase. The company is writing or updating its SSP across all applicable control families, developing the POA&M for residual risks, creating or formalizing security policies and SOPs, and implementing technical controls (SIEM, vulnerability scanning, FIPS 140-2/3 encryption, MFA, etc.). For 20x pathway companies, this phase focuses on codifying compliance into infrastructure automation and building the persistent validation pipeline rather than writing narrative SSP documents.

> **Example:** The company hires a GRC lead, implements a SIEM solution, establishes automated vulnerability scanning on a 30-day cadence, and begins drafting SSP control narratives. The POA&M tracks 12 remaining items with target remediation dates.

5 Agency Sponsor Secured (or Sponsorless Pathway Initiated)

The company has secured a federal agency sponsor, qualified for Program Authorization, or submitted a 20x validation package — and the authorization package is under formal review.

Under the post-JAB model, this milestone can take one of three forms: Agency Authorization (agency agrees to sponsor), Program Authorization (FedRAMP Director reviews for widely-used services without sponsors), or FedRAMP 20x (CSP submits validation package directly to the PMO for assessment in as little as 30 days). The FedRAMP 20x Phase 1 pilot (Low) ran April–September 2025, granting authorizations to 12 participants. Phase 2 (Moderate) ran through March 2026, and Phase 3 (wide-scale adoption) is expected mid-to-late 2026.

> **Example:** HHS agrees to sponsor the startup's FedRAMP Moderate authorization after a successful pilot deployment. The complete package is submitted to the agency's CISO office for review. Alternatively, a cloud-native startup with strong automation capabilities submits a FedRAMP 20x Low package and receives initial feedback from the PMO within 3 weeks.

6 3PAO Assessment Complete (or 20x Validation Assessed)

The full 3PAO security assessment has been completed and the SAR delivered, or the PMO has completed its assessment of the 20x validation package.

Under Rev 5, the 3PAO tests all applicable controls, reviews documentation, performs penetration testing, and produces the SAR. Under 20x, the PMO assesses the CSP's persistent validation processes, KSI automation, vulnerability detection and response posture, and authorization data sharing capabilities. Findings are documented and the company is addressing them before the authorization decision.

> **Example:** The 3PAO completes its Rev 5 assessment over 6 weeks, testing 325 controls. The SAR identifies 8 findings — 2 High, 4 Moderate, 2 Low. The company remediates both High findings within 30 days and documents risk acceptance rationale for the Moderate findings in the POA&M.

7 Authority to Operate Granted

The AO (Agency Auth), FedRAMP Director (Program Auth), or PMO (20x) has issued the authorization. The system is FedRAMP Authorized.

Under the unified model, there is one designation: **FedRAMP Authorized**. The former "JAB P-ATO" vs. "Agency ATO" distinction no longer exists. Rev 5 authorizations receive a "FedRAMP Certified" designation; 20x authorizations receive "FedRAMP Validated" — reflecting persistent, automation-driven validation. Both mean the service is FedRAMP Authorized and available for agency reuse.

> **Example:** The agency's AO signs the authorization, and the company achieves FedRAMP Certified (Rev 5) Moderate status. The system is listed on the FedRAMP Marketplace. Continuous monitoring obligations begin immediately.

8 Marketplace Listed and Multi-Agency Reuse

The authorization is on the FedRAMP Marketplace, and additional agencies are leveraging the existing authorization for their own deployments.

The company's authorization enables other agencies to reuse the package rather than conducting full assessments. Collaborative Continuous Monitoring (ConMon) enables multiple agencies to share oversight. Each reusing agency may issue its own ATO with agency-specific additions.

> **Example:** After achieving FedRAMP Moderate through HHS, the company is adopted by the VA and Department of Education. Each issues their own agency ATO leveraging the FedRAMP package, adding 2 new production deployments within 6 months.

9 Sustained Authorization and Pathway Evolution

The company maintains authorization across multiple agencies, operates mature continuous monitoring, and is adapting to evolving FedRAMP requirements (Rev 5 to 20x transition).

FedRAMP is internalized as a core business operation. The company proactively manages annual assessments, significant change requests, and POA&M remediation. It is preparing for the Rev 5 to 20x transition — FedRAMP aims to stop accepting new Rev 5 packages by FY27 Q3–Q4. The authorization is a durable competitive moat in both government and commercial sales.

> **Example:** The company holds active authorizations across 7 federal agencies, operates automated ConMon from its CI/CD pipeline, and has begun transitioning from Rev 5 Certified to 20x Validated status. Its FedRAMP authorization contributes to commercial wins in healthcare and financial services.

DoD RMF Authorization Readiness Level (RARL)

The DoD RMF Authorization Readiness Level assesses progress in achieving ATO under the Department of Defense Risk Management Framework, implemented through eMASS and governed by DoDI 8510.01, NIST 800-53 Rev 5, CNSSI 1253, and DISA STIGs.

1 Mission Need and RMF Awareness

The company understands that DoD deployment requires RMF authorization and has begun learning DoD-specific requirements beyond commercial frameworks.

The company recognizes that DoD authorization differs fundamentally from SOC 2, ISO 27001, and even FedRAMP. It is learning about eMASS, DISA STIGs, the AODR role, and the six-step RMF process (Categorize, Select, Implement, Assess, Authorize, Monitor).

> **Example:** A dual-use AI analytics company has been approached by a DoD program office. The CISO begins studying DoDI 8510.01, recognizing the company will need an eMASS record, STIG compliance, and a DoD-specific ATO.

2 System Categorization and eMASS Registration

The system has been categorized using CNSSI 1253, and an eMASS record has been initiated with the sponsoring organization.

> **Example:** Working with the Defense Health Agency, the company categorizes its system as Moderate-Moderate-Low. An eMASS record is created and the NIST 800-53 Moderate baseline is selected with DHA-specific overlays.

3 STIG Assessment and Control Implementation Planning

Applicable DISA STIGs have been identified, compliance assessed, and an implementation plan developed for both STIG and NIST 800-53 controls.

> **Example:** The company runs STIG assessments across RHEL 8, PostgreSQL, and Apache. Of 847 checks, 612 pass, 187 require remediation, and 48 need documented mitigations. A 90-day sprint plan is built.

4 Security Documentation Development in eMASS

The full RMF documentation package is being developed within eMASS — SSP, control narratives, and supporting artifacts.

> **Example:** The compliance team works through 325 NIST 800-53 controls in eMASS, prioritizing CM and SA families given the software-defined architecture. POA&M items are entered for controls not yet satisfied.

5 Security Control Assessor (SCA) Engagement

An independent SCA has been engaged to conduct the formal assessment.

> **Example:** DHA's SCA team reviews the eMASS package and develops a Security Assessment Plan. The company conducts internal dry runs and strengthens 6 controls with weak evidence.

6 Security Assessment Complete

The SCA has completed the formal assessment, the SAR is generated in eMASS, and findings have been adjudicated.

> **Example:** The SCA identifies 23 findings — 1 CAT I, 14 CAT II, 8 CAT III. The CAT I is remediated within 2 weeks. Remaining findings are documented in the POA&M and the package is submitted to the AO.

7 Authority to Operate Granted

The AO has signed the ATO, authorizing the system for operation within the DoD environment.

> **Example:** DHA's AO signs a 3-year ATO with conditions: remediate all CAT II items within 180 days and maintain monthly ConMon through eMASS. The system is cleared for production deployment.

8 Operational ATO with Active Continuous Monitoring

The system is in production, and authorization is maintained through active ConMon, POA&M management, and ongoing STIG compliance.

> **Example:** Monthly ConMon reports flow through eMASS. Automated STIG checks run after each change. When DISA releases an updated RHEL 8 STIG, the team assesses within 30 days.

9 Multi-Enclave Authorization and RMF Maturity

Active ATOs across multiple DoD organizations, repeatable RMF processes, and efficient reciprocity-based expansion.

> **Example:** After DHA ATO, the company pursues DLA and USCYBERCOM. Leveraging 80% of existing artifacts, each subsequent ATO takes 6 months instead of 18. A centralized GRC platform tracks all enclaves.

Impact Level Authorization Readiness Level (IARL)

The IARL assesses progress toward Provisional Authorization (PA) at DoD Impact Levels 4, 5, or 6 under the CC SRG. This pathway is managed by DISA — distinct from FedRAMP (managed by the FedRAMP PMO at GSA). While both build on NIST 800-53, the IL PA process adds DoD-specific isolation, encryption, personnel, and incident reporting requirements.

1 Impact Level Strategy and Applicability Determination

The company understands the IL framework (IL2–IL6+) and has determined which IL its product must achieve.

> **Example:** A collaboration platform determines DoD customers need to process CUI including ITAR data, requiring IL5. The company evaluates building IL5 infrastructure vs. leveraging an existing IL5-authorized IaaS provider.

2 Infrastructure and Isolation Architecture Design

Cloud architecture is designed for IL-specific isolation, encryption, and geographic requirements.

> **Example:** The company designs an IL5 architecture on AWS GovCloud — dedicated VPCs, FIPS 140-3 encryption, CONUS-only data centers, no public internet exposure.

3 CC SRG Gap Assessment

Gap assessment completed against CC SRG requirements, identifying the delta beyond FedRAMP Moderate.

> **Example:** The gap analysis identifies 38 additional requirements beyond FedRAMP Moderate, including US person restrictions, USCYBERCOM incident reporting, and physical isolation.

4 DISA Engagement and PA Application

DISA formally engaged and PA application submitted or in preparation.

> **Example:** The company submits its IL5 PA application to DISA with its FedRAMP package, CC SRG remediation docs, and a sponsoring DoD component letter of need.

5 DISA Assessment In Progress

DISA's assessment team is actively evaluating the system against CC SRG requirements.

> **Example:** DISA conducts a 3-month evaluation including facility inspection, FIPS module testing, and US person access verification. Five findings are identified.

6 Assessment Complete and Findings Remediated

DISA assessment complete, findings remediated or in POA&M, package pending PA decision.

> **Example:** All 5 findings remediated within 60 days. Two remaining low-risk items documented with 90-day POA&M timelines approved by DISA.

7 Provisional Authorization Granted

DISA has granted PA at the target Impact Level. The company is authorized to host DoD workloads.

> **Example:** DISA grants IL5 PA. The platform is added to the DoD Cloud Computing Catalog. The sponsoring component begins migrating CUI workloads immediately.

8 Production Operations at Impact Level with ConMon

DoD workloads are running at IL; the company maintains continuous compliance with CC SRG requirements.

> **Example:** Production CUI workloads for 4 DoD organizations run on IL5 infrastructure. Monthly ConMon to DISA. Dedicated SOC with US person staff.

9 Multi-IL Authorization and Strategic Positioning

PAs held at multiple ILs; the authorization portfolio is a strategic differentiator and competitive moat.

> **Example:** The company holds IL4 and IL5 PAs and is pursuing IL6. Multi-IL capability enables DoD customers to scale from CUI to classified without changing platforms.

Continuous ATO Readiness Level (CARL)

The CARL assesses progress toward a Continuous Authority to Operate (cATO) — replacing the traditional 3-year ATO cycle with continuous, automated security monitoring and risk-based authorization decisions. Aligned with the DoD Enterprise DevSecOps Reference Design, SWFT, and the Platform One / Iron Bank ecosystem.

1 DevSecOps Foundation and cATO Awareness

The company has a CI/CD pipeline and understands the cATO model requires integrating security into the delivery lifecycle.

> **Example:** A DevSecOps platform company has a mature GitLab CI / Kubernetes pipeline. The CTO reads the DoD Enterprise DevSecOps Reference Design and recognizes the pipeline needs automated scanning, SBOM generation, and continuous compliance checking.

2 Security Tooling Integration into CI/CD

Automated security scanning (SAST, DAST, SCA, container scanning) integrated into the pipeline; SBOM generation automated.

> **Example:** SonarQube, OWASP ZAP, Anchore, and Syft/Grype are integrated into the pipeline. Every merge request triggers scans. Critical/High vulnerabilities block promotion to production.

3 Continuous Monitoring Architecture

Real-time continuous monitoring with automated compliance checking against NIST 800-53 and DISA STIGs.

> **Example:** OpenSCAP for STIG checks, Elastic Security SIEM mapped to AU and SI control families, real-time compliance dashboard. Configuration drift detected and auto-remediated within 15 minutes.

4 Hardened Container Pipeline and Artifact Provenance

Hardened base images (Iron Bank or equivalent), cryptographically signed artifacts, full provenance from source to production.

> **Example:** All base images migrated to Iron Bank equivalents. Every image signed with Cosign, SBOMs attached as attestations, full provenance chain from Git commit to running container.

5 DoD Program Sponsor Engagement for cATO

A DoD program office is willing to sponsor a cATO, with agreed-upon shared responsibilities and governance.

> **Example:** An Air Force program office agrees to sponsor the cATO. Metrics agreed: daily automated compliance reports, vulnerability SLAs (Critical: 48 hours, High: 7 days), quarterly risk reviews replacing 3-year reauthorization.

6 Initial cATO Assessment and Authorization

The AO has assessed the DevSecOps pipeline and monitoring capabilities and issued a cATO (or ATO with cATO conditions).

> **Example:** After a 4-week assessment, the AO issues a cATO with a 90-day probationary period. The ISSM reviews daily automated reports and conducts two spot-check assessments.

7 Operational cATO with Automated Compliance Reporting

Active cATO with continuous automated compliance data flowing to the AO; software ships without per-release authorization.

> **Example:** Production releases ship 3 times per week through automated security gates. The ISSM receives daily dashboards. No manual authorization review for individual releases.

8 Mature cATO Operations and Multi-Program Expansion

cATO proven over multiple cycles; additional DoD programs adopting the product under the same or parallel cATO arrangements.

> **Example:** After 18 months of cATO operations, deployment extends to 3 additional squadrons. A separate Army program completes its cATO assessment in just 3 weeks.

9 Enterprise cATO and DevSecOps Reference Implementation

The cATO model and pipeline are recognized as reference implementations; the company contributes to DoD DevSecOps standards.

> **Example:** The pipeline is cited in a DoD CIO memo as a cATO reference. The company contributes hardened containers to Iron Bank, participates in DoD working groups, and briefs at the DevSecOps Symposium.

CMMC Readiness Level (CMRL)

The CMMC Readiness Level assesses a defense contractor's progress toward achieving Cybersecurity Maturity Model Certification under CMMC 2.0. Following the publication of the 32 CFR final rule (October 15, 2024) and the DFARS 252.204-7021 rule (effective November 10, 2025), CMMC certification is transitioning from aspirational to mandatory across the defense industrial base. The framework covers three certification levels: Level 1 (15 FAR 52.204-21 controls for FCI), Level 2 (110 NIST SP 800-171 Rev 2 controls for CUI, requiring C3PAO assessment for most contracts), and Level 3 (Level 2 plus 24 select NIST SP 800-172 controls, assessed by DIBCAC for highest-sensitivity programs). With an estimated 80,000 contractors needing Level 2 certification and fewer than 600 Certified CMMC Assessors available, the bottleneck is real — an estimated 33,000–44,000 companies may exit the defense market between 2025–2027. *Note on NIST 800-171 Revision:* NIST published SP 800-171 Rev 3 in May 2024, but CMMC 2.0 as codified in 32 CFR remains aligned to **Rev 2** (110 controls). The DoD issued a class deviation postponing the Rev 3 transition; premature adoption of Rev 3 controls can result in assessment deficiencies. Future rulemaking will formally transition CMMC to Rev 3, likely no earlier than 2027–2028. This framework references Rev 2 throughout to reflect current assessment requirements.

1 CMMC Awareness and Level Determination

The company understands that CMMC certification is required for its defense contracts and has determined whether it handles FCI (Level 1), CUI (Level 2), or high-sensitivity CUI (Level 3).

At this level, the company is mapping its contractual requirements to CMMC levels. It is reviewing DFARS clauses in existing and anticipated contracts, identifying whether data it handles qualifies as FCI or CUI under the CUI Registry, and understanding the phased rollout timeline. Leadership recognizes that CMMC is not optional — Phase 1 began November 10, 2025, and failing to certify means losing contract eligibility.

> **Example:** A dual-use AI analytics company reviews its DoD contracts and identifies CUI markings on data it processes. The CISO determines CMMC Level 2 certification with C3PAO assessment will be required by Phase 2 (November 2026). The company begins budgeting for the certification effort.

2 Scoping and CUI Asset Identification

The company has defined its CUI boundary, identified all systems and assets that process, store, or transmit CUI, and documented CUI data flows.

The company has conducted a thorough scoping exercise to identify its CUI environment — the people, processes, and technology that interact with Controlled Unclassified Information. CUI enclaves are defined, data flow diagrams map how CUI enters, moves through, and exits the organization, and the assessment scope is clearly bounded. This scoping directly determines the effort and cost of achieving certification.

> **Example:** The company maps CUI data flows across its development, staging, and production environments. It identifies 3 systems in scope, isolates CUI processing into a dedicated enclave, and determines that 2 SaaS tools used by engineering also handle CUI and must be included in the assessment boundary.

3 NIST 800-171 Gap Assessment and SPRS Score

A formal gap assessment against all 110 NIST SP 800-171 Rev 2 controls has been completed, and the company has calculated and submitted its SPRS score.

The company has methodically evaluated its security posture against each of the 110 controls in NIST 800-171. A SPRS (Supplier Performance Risk System) score has been calculated using the DoD methodology and submitted. The gap assessment provides a clear picture of which controls are fully implemented, partially implemented, or not implemented, along with the remediation effort required for each gap.

> **Example:** The gap assessment reveals the company meets 72 of 110 controls, with a SPRS score of -88 (out of 110). Major gaps exist in audit and accountability (AU), configuration management (CM), and incident response (IR). The company builds a prioritized remediation plan targeting the 38 unmet controls.

4 SSP Development and Control Implementation

The company is actively building its System Security Plan, implementing remediation for unmet controls, and closing gaps identified in the assessment.

This is the heavy-lift phase. The company is writing its SSP documenting how each of the 110 controls is implemented, developing supporting policies and procedures, and implementing technical and operational controls to close gaps. For companies pursuing Level 3, this also includes implementing the 24 additional NIST SP 800-172 controls. POA&Ms are being developed for controls that cannot be immediately remediated, but must meet the strict CMMC limitations — no POA&Ms allowed for Level 1, and Level 2/3 POA&Ms are limited to non-critical controls with 180-day closeout requirements.

> **Example:** The company implements a SIEM for audit log centralization, deploys endpoint detection and response (EDR) across all CUI-processing endpoints, establishes a formal incident response plan, and documents control implementations in a comprehensive SSP. 8 remaining gaps are documented in POA&Ms with 90-day remediation targets.

5 POA&M Closeout and Assessment Readiness

All critical control gaps have been remediated, POA&Ms are within allowable limits, evidence packages are assembled, and the company is ready for formal assessment.

The company has closed out the majority of its POA&Ms and confirmed that any remaining items meet CMMC requirements (limited to specific non-critical controls, with 180-day closeout windows). Evidence packages have been prepared for each control — screenshots, configuration exports, policy documents, interview preparation guides. The company has conducted internal mock assessments or engaged a Registered Practitioner Organization (RPO) for pre-assessment readiness review.

> **Example:** The company closes 35 of 38 POA&M items. The 3 remaining items are verified as eligible for POA&M under CMMC rules. A mock assessment conducted by an RPO identifies 4 evidence gaps that are corrected in 2 weeks. The company formally engages a C3PAO for Level 2 assessment.

6 C3PAO Assessment Complete

The formal C3PAO assessment (or self-assessment for Level 1/Level 2-Self; DIBCAC assessment for Level 3) has been completed, findings adjudicated, and the assessment report submitted.

For most CUI-handling contracts, a Certified Third-Party Assessment Organization (C3PAO) conducts the formal Level 2 assessment, evaluating evidence for all 110 NIST 800-171 controls. For Level 1 and select Level 2 contracts, self-assessment with senior official affirmation is permitted. For Level 3, the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) conducts the assessment after C3PAO Level 2 is achieved. Any identified deficiencies must be remediated or documented in allowable POA&Ms before certification can be issued.

> **Example:** The C3PAO conducts a 5-day on-site assessment, evaluating all 110 controls across the scoped environment. The assessment identifies 3 deficiencies — 2 are remediated on-site during the assessment, and 1 is documented as an allowable POA&M. The C3PAO submits the assessment results to the CMMC PMO.

7 CMMC Certification Achieved

CMMC certification has been issued, the CMMC Unique Identifier (UID) is recorded, status is reflected in SPRS, and the company is eligible for contract award.

The CMMC PMO has reviewed the assessment results and issued the certification. The company's certification status is recorded in SPRS and linked to its CAGE code. For Level 2, the certification is valid for 3 years with annual affirmation required. The company can now compete for and be awarded contracts requiring CMMC certification at the achieved level. Any POA&Ms from the assessment must be closed within 180 days to maintain certification.

> **Example:** CMMC Level 2 certification is issued 6 weeks after the C3PAO assessment submission. The company's SPRS record reflects certified status. Within 30 days, the company is included in 3 new RFP responses that require CMMC Level 2 certification. The remaining POA&M item is remediated within 60 days.

8 Operational Compliance and Annual Affirmation

The company maintains continuous CMMC compliance, completes required annual affirmations, manages subcontractor flowdown requirements, and integrates CMMC into ongoing operations.

Certification is not a one-time event. The company has integrated CMMC compliance into its operational rhythm — continuous monitoring of the 110 controls, annual affirmation by a senior company official attesting continued compliance, POA&M management for any new deficiencies discovered through ongoing operations, and flowdown of appropriate CMMC requirements to subcontractors handling CUI. The company proactively manages CUI boundary changes as its environment evolves.

> **Example:** The CISO completes the annual affirmation in SPRS 10 months after certification. Quarterly internal audits verify control effectiveness. When a new SaaS tool is introduced into the CUI environment, the company updates its SSP and boundary documentation within 30 days. Subcontractors are verified for appropriate CMMC level before CUI is shared.

9 Multi-Level Certification and DIB Leadership

The company holds certifications at multiple CMMC levels (Level 2 + Level 3), manages a mature supply chain compliance program, and leverages its certification as a competitive differentiator across the defense industrial base.

The company has achieved the highest applicable CMMC levels and manages certification as a strategic asset. For companies pursuing Level 3, DIBCAC assessment has been completed on top of C3PAO Level 2

certification. The company actively manages its supply chain CMMC posture, assists key subcontractors in achieving certification, and positions its CMMC maturity as a competitive moat. With an estimated 33,000–44,000 companies expected to exit the defense market due to CMMC requirements, certified companies gain significant market share.

> **Example:** The company holds Level 2 certification across 3 divisions and has achieved Level 3 for its highest-sensitivity program. It operates a subcontractor compliance portal that tracks CMMC status across 45 suppliers. The CMMC certification is prominently featured in proposals and has directly contributed to 4 contract wins where competitors lacked certification. The company is invited to participate in the CMMC stakeholder forum.

Mapping Authorization Readiness to MIT's Dual-Use Readiness Levels

Authorization Readiness Levels interact with every dimension of MIT's framework. The following mapping shows typical alignment:

AUTHORIZATION STAGE	TYPICAL MIT ALIGNMENT	KEY IMPLICATION
ARL 1–2 (Awareness, Scoping)	TRL 4–5, MFRL 1–2, MCRL 1–2	Architecture decisions must be made with authorizability in mind. Most cost-effective time to design for compliance.
ARL 3–4 (Gap Analysis, Remediation)	TRL 6–7, MFRL 3–4, MCRL 3–4	Compliance remediation should be funded — SBIR Phase II, OTA, or seed/Series A should include ATO budget. Expect $500K–$2M for Rev 5; potentially much less under 20x.
ARL 5–6 (Assessment)	TRL 7–8, MFRL 5–6, MCRL 5–6	The AO is a mission customer. Managing the assessment relationship is as important as the technology itself.
ARL 7 (ATO Granted)	TRL 8–9, MFRL 7, MCRL 7–8	Authorization unlocks production revenue. The inflection point for mission customer conversion.
ARL 8–9 (ConMon, Multi-Agency)	TRL 9, MFRL 8–9, MCRL 8–9, CFRL 6+	Sustained authorization is a competitive moat. Investors value it. Reuse and reciprocity accelerate growth.

Key Principles for Dual-Use ATO Strategy

1. Design for Authorization from Day One

The most expensive ATO decision is the one you don't make early enough. Selecting a FedRAMP-authorized IaaS provider, implementing FIPS-validated encryption, and designing your system boundary at TRL 3–5 saves 6–12 months and hundreds of thousands of dollars compared to retrofitting at TRL 7–8.

2. The AO Is a Customer, Not a Gatekeeper

The Authorizing Official and their team (ISSM, ISSO, SCA) are mission customer stakeholders. Build relationships early, understand their risk appetite, and treat the process as a partnership.

3. Fund Authorization Like a Product Feature

ATO is not overhead — it is a product feature that unlocks an entire market. Budget for it in SBIR proposals, include it in OTA milestones, and present it to investors as go-to-market infrastructure. A $1.5M FedRAMP investment that unlocks $50M in addressable government revenue is a 33x leverage play.

4. Leverage Inheritance and Reciprocity

Build on FedRAMP-authorized IaaS/PaaS to inherit 50–70% of the control baseline. Leverage reciprocity between DoD organizations. Use your FedRAMP authorization as the foundation for DoD RMF and IL authorization.

5. Build Toward Continuous, Not Just Compliant

FedRAMP 20x replaces narrative SSPs with machine-readable KSIs and persistent validation. DoD cATO replaces 3-year cycles with continuous monitoring. FedRAMP aims to stop accepting new Rev 5 packages by late FY27 — the transition window is now.

6. Treat Authorization as a Competitive Moat

Every additional agency ATO, every IL level, every year of ConMon history widens the moat. Protect and maintain your authorizations — they are among your most valuable business assets.

7. Understand the Institutional Map

FedRAMP is managed by the **FedRAMP PMO at GSA**, with strategy set by the **FedRAMP Board**. IL Provisional Authorizations are managed by **DISA** under the CC SRG — a separate process. DoD RMF ATOs are issued by **individual DoD AOs** and tracked through **eMASS**. CMMC certifications are managed by the **CMMC PMO** with assessments conducted by **C3PAOs** and **DIBCAC**. Understanding which institution owns which authorization prevents wasted effort.

Beyond Authorization: Procurement Blockers Dual-Use Companies Must Navigate

Authorization to operate is necessary but not sufficient. Even after achieving ATO, dual-use companies face a gauntlet of procurement, contractual, and institutional barriers that can delay or prevent production revenue. Authorization readiness must be paired with procurement readiness.

The Valley of Death: From Pilot to Production Contract

The most dangerous gap in defense technology commercialization remains the transition from prototype funding (SBIR Phase II, OTA prototyping) to production contract. STRATFI (Strategic Funding Increase, $3M–$15M) and TACFI (Tactical Funding Increase, $375K–$2M) were designed to bridge this gap for SBIR/STTR awardees, but data shows more than half of completed projects still die in transition — usually because funding priorities shift, not because the technology failed. Compounding the problem, SBIR/STTR program authorization expired on October 1, 2025, pausing new activity while Congress debates reauthorization. Companies relying on the SBIR pipeline for DoD entry should have contingency acquisition strategies.

Contract Vehicle Access

Having an ATO does not mean an agency can easily buy your product. Federal procurement flows through contract vehicles — pre-competed mechanisms like GWACs (Government-Wide Acquisition Contracts), IDIQs, and GSA MAS (Multiple Award Schedule). Without access to the right vehicle, even an authorized

product may be unreachable to a willing buyer. Key vehicles for software companies include OASIS+ (professional services), the forthcoming JWCC Next (enterprise cloud, expected solicitation in FY26 Q2 with award in early 2027), and agency-specific BPAs and IDIQs. Startups that lack their own vehicle access must build strategic teaming relationships with primes who hold seats on relevant contracts.

Security Clearances and Facility Requirements

For classified programs (IL6+, SAP/SCI environments), company personnel need active security clearances and the company needs a Facility Security Clearance (FCL) managed through DCSA (Defense Counterintelligence and Security Agency). Obtaining a sponsorship for an FCL requires an existing classified contract or a bona fide need letter — a chicken-and-egg problem for startups. Cleared facility requirements (SCIF/SAPF access) add capital expense and timeline that many early-stage companies underestimate.

ITAR and Export Control Compliance

Companies whose products touch defense articles, technical data, or defense services must register with the Directorate of Defense Trade Controls (DDTC) and comply with the International Traffic in Arms Regulations (ITAR). Non-compliance can result in contract disqualification, civil penalties, or criminal prosecution. For dual-use companies with international customers or development teams, ITAR creates real architectural constraints — foreign national access must be controlled, development environments may need to be segregated, and cloud infrastructure must meet ITAR storage requirements.

The Software Fast Track (SWFT) Initiative

Launched via an April 2025 memo from the Acting DoD CIO, SWFT seeks to accelerate software acquisition by replacing the traditional RMF process with AI-enabled continuous compliance workflows, standardized use of SBOMs, and independent third-party software security assessments. SWFT entered a 90-day sprint on June 1, 2025, with active RFIs to industry. While SWFT is not yet a production pathway, it signals the DoD's intent to converge ATO and acquisition timelines — companies investing in DevSecOps automation and continuous authorization (CARL 5+) are best positioned to benefit.

FY2026 NDAA Acquisition Reforms

The FY2026 National Defense Authorization Act introduced significant procurement reforms relevant to dual-use companies. Section 1822 now requires contracting officers to use commercial procurement pathways unless they formally determine that no suitable commercial alternative exists — a structural shift toward commercial-first acquisition. The NDAA also increases critical acquisition thresholds, expands OTA authority,

and overhauls the major systems acquisition lifecycle toward a portfolio-based model. These reforms lower barriers for non-traditional contractors but require companies to understand the new landscape.

Procurement Consolidation

Executive direction in 2025 centralized domestic procurement of common goods and services within GSA, with agency-specific IDIQs expected to retire at recompete in favor of GSA MAS or GWAC usage. This consolidation simplifies the vehicle landscape for new entrants but also means companies need GSA Schedule or GWAC access to reach the broadest set of federal buyers.

FedRAMP Authorization Landscape: Key Changes (2024–2026)

JAB Dissolution (August 2024): The JAB was dissolved per OMB Memo M-24-15. The JAB P-ATO designation no longer exists. All authorizations are now simply "FedRAMP Authorized." Governance transferred to the new FedRAMP Board.

Unified Authorization Model: One status — FedRAMP Authorized — achieved through Agency Authorization, Program Authorization (sponsorless), or FedRAMP 20x Validation.

FedRAMP 20x Phased Rollout:

- Phase 1 (Low pilot, Apr–Sep 2025): 26 CSPs submitted; 12 received pilot authorizations
- Phase 2 (Moderate pilot, through Mar 2026): 13 participants across two cohorts
- Phase 3 (wide-scale adoption, FY26 Q3–Q4): Formalizes 20x Low and Moderate; opens broadly
- Phase 4 (FY27 Q1–Q2): Pilots 20x High authorization
- Phase 5 (FY27 Q3–Q4): Target to stop accepting new Rev 5 packages

New Designations (RFC-0020, ~March 2026): FedRAMP Certified (Rev 5) and FedRAMP Validated (20x). Both = FedRAMP Authorized.

Sponsorless Pathway (RFC-0023, January 2026): Rev 5 Program Certification without agency sponsor. FedRAMP Ready phasing out — no new submissions after July 2026.

Conclusion

The pathway to Authority to Operate is the hidden dimension of dual-use strategy. MIT's Dual-Use Readiness Levels™ framework provides an excellent foundation for understanding startup maturity across technology, funding, and customer dimensions. The Authorization Readiness Levels extend that foundation into the critical domain of security authorization — the domain that ultimately determines whether a dual-use product reaches production in the defense and public sector markets.

For founders: use these levels to assess where you are, plan where you need to go, and communicate your authorization strategy to investors and government stakeholders with precision and credibility.

For investors: use these levels to evaluate authorization maturity and understand the timeline and investment required to unlock government revenue.

For government stakeholders: use these levels to understand where your vendor partners are in their authorization journey and what they need — sponsorship, assessment resources, AO engagement — to advance.

The companies that master both sides of dual-use — commercial and mission — while also mastering the authorization dimension will be the ones that define the next generation of defense technology.

ABOUT THE AUTHOR

Ryan Gutwein is the founder/CEO of Optimal Labs, Inc. and Optimal, LLC (CAGE: 14HQ0). He is a nine-year Air Force veteran (Security Forces), holds active FedRAMP 3PAO assessment contracts, scored 449/500 on his CCA exam, and has deep operational experience across FedRAMP, DoD RMF/eMASS, DISA STIGs, CMMC, and DevSecOps.

This framework was authored by Ryan Gutwein as a companion to MIT's Dual-Use Readiness Levels™. It draws on operational experience across FedRAMP 3PAO assessment, DoD RMF authorization, DISA STIG compliance, CMMC certification, and DevSecOps continuous authorization.

MIT's Dual-Use Readiness Levels™ is a trademark of the Massachusetts Institute of Technology. This document references the MIT framework with attribution and is not

affiliated with or endorsed by MIT.

© 2026 Ryan Gutwein. All rights reserved.