WHITE PAPER · VERSION 1.0 · SEPTEMBER 2026

Custody of Controlled Technical Information

A practical model for inventory, chain of custody, flow-down, and verifiable evidence under DFARS 252.204-7012, NIST SP 800-171, and DoW Instruction 8430.01

The Department of War has spent a decade discovering it cannot see what its contractors hold. This paper explains how a small or mid-size defense contractor can know where its CTI is, prove who touched it, and produce that proof in the form the department is now writing into policy.

Eddie White

CMMC Registered Practitioner · ISO 9001 Lead Auditor · Lean Six Sigma Master Black Belt
Founder and Principal Consultant, Globe-America Consulting, Inc.

Service-Disabled Veteran-Owned Small Business · Fort Worth, Texas · CAGE 8LQR6 · globe-america.com

Executive Summary

Most defense contractors can describe their cybersecurity program. Far fewer can answer three questions about Controlled Technical Information (CTI) without a week of reconstruction: What do we hold? Where is it right now? Who has touched it? Those three questions are the substance of custody, and custody is the control the Department of War (DoW) has repeatedly discovered it cannot verify across its supply chain.

The evidence is public. In May 2023 the Government Accountability Office reported that one F-35 prime contractor had lost more than one million spare parts worth over 85 million dollars since 2018, that the F-35 Joint Program Office had reviewed less than two percent of those losses, and that the reason was structural: the government did not track the parts in its own system of record, so the contractor's records were the only records (GAO-23-106098). In September 2026 the same weakness produced a national security story when a shipment of unserviceable F-35 components, including a canopy incorporating low-observable technology, was diverted to Hong Kong in transit from Australia and the department could not say where it was. Eleven days earlier, the DoW Chief Information Officer had signed DoW Instruction 8430.01, which declares software artifacts with a military application to be CTI at inception and requires machine-readable evidence the government can verify itself rather than records it has to request. And on September 1, 2026, the Department of Justice settled False Claims Act allegations with Honeywell Aerospace over NIST SP 800-171 gaps that predate any CMMC clause, during the period in which CMMC Phase 2 was suspended.

Read together, those four facts describe a direction, not a set of isolated events. The department is replacing trust in contractor-controlled records with evidence it can pull on demand. That shift is arriving through policy, enforcement, and prime flow-downs faster than through any single rule, and it will not wait for the CMMC Reform Task Force.

This paper gives a contractor handling CTI a working model for custody organized around four questions, Know, Locate, Prove, and Flow, mapped to the four phases of the Cyber G.A.R.D. Framework and to the specific NIST SP 800-171 requirements, DFARS clauses, and 8430.01 paragraphs that make each question a contractual obligation. It closes with a ninety-day roadmap and a self-check a contractor can run this week.

> **The one-sentence version**
>
> If a contracting officer, a DIBCAC assessor, or a prime asked you tomorrow to show where every piece of your CTI is and who has handled it, you should be able to produce evidence, not a narrative. Everything in this paper is in service of that sentence.

1. The Problem: Custody Without Visibility

Every CTI protection regime the department has issued since 2013 rests on the same premise: the contractor knows what it has and where it is. DFARS 252.204-7012 requires adequate security for covered defense information on covered contractor information systems; the clause is meaningless if the contractor cannot identify which information and which systems are covered. NIST SP 800-171

opens with a scoping requirement for exactly that reason. CMMC's asset categorization rules in 32 CFR 170.19 exist because assessors learned that the boundary, not the controls, is where most programs fail.

Three recent events show what happens when the premise is false.

1.1 The F-35 spare parts finding (GAO-23-106098, May 2023)

GAO found that the F-35 Joint Program Office did not oversee or account for spare parts in the global spares pool that were located at non-prime contractor facilities, and did not track them in an accountable property system of record. The prime contractors maintained that information. Because the program office had no complete record of losses, GAO had to combine program office data with data from one prime to reach a count: over one million parts lost since May 2018, over 85 million dollars in value, less than two percent reviewed by the government, and more than 900,000 additional parts worth over 66 million dollars never reported for review because no reporting process existed. The underlying dispute, whether the parts were government-furnished property at all, had been unresolved since 2015.

The point is not the dollar figure. It is that the department could not audit the loss because the only records were the contractor's, and the contractor's records were incomplete in ways the contractor did not have to disclose.

1.2 The F-35 shipment diversion (September 2026)

On September 18, 2026, Politico reported that a shipment of unserviceable F-35 components moving from Australia to the United States for repair had been rerouted in transit and ended up in Hong Kong. The shipment was handled by an intermediary on behalf of the prime. It reportedly included a cockpit canopy incorporating low-observable technology. The F-35 Joint Program Office confirmed a shipment issue and said it was working with U.S. authorities and industry partners to recover the components. As of this writing it has not been established why the diversion occurred, whether it was error or intent, or who holds the parts. State Department and Pentagon officials briefed congressional committees beginning in June.

The diversion is also an export-control matter: F-35 components are defense articles under ITAR, and Hong Kong has been treated as mainland China for export purposes since 2020. That question belongs to the State Department and the parties. For this paper the relevant fact is narrower. Custody records lived in contractor and intermediary systems, and when routing failed, the government learned late and could not answer the location question.

1.3 Enforcement during the CMMC pause (September 2026)

On July 13, 2026 the DoW suspended the transition to CMMC Phase 2 and stood up a Reform Task Force. On September 3 a class deviation made the suspension binding on contracting officers. On September 1, between those two dates, the Department of Justice announced a two million dollar False Claims Act settlement with Honeywell Aerospace over alleged NIST SP 800-171 noncompliance on a defense contract between 2020 and 2023. No CMMC assessment clause existed in that period. The government enforced through DFARS 7012 and the FCA, the same path it used against Aerojet Rocketdyne in 2022 for nine million dollars.

The lesson for a contractor is that the certification gate and the obligation are separate things. The gate moved. The obligation, and the enforcement behind it, did not.

> **What these three events have in common**
>
> In each case the government's ability to verify depended on records it did not control. GAO could not audit losses. The Pentagon could not locate a canopy. DOJ had to reconstruct a contractor's 800-171 posture from three-year-old evidence. The department's response, visible in DoW Instruction 8430.01, is to stop depending on those records.

2. What Custody Covers: CUI, CTI, and Where It Actually Lives

Custody is only as good as the inventory it rests on, and most inventories are too narrow. The following definitions and locations are the ones that matter.

2.1 Definitions that drive scope

- **Controlled Unclassified Information (CUI).** Information the government creates or possesses, or that an entity creates or possesses on the government's behalf, that a law, regulation, or government-wide policy requires or permits an agency to safeguard. Governed by 32 CFR Part 2002 and, within the DoW, DoDI 5200.48.
- **Controlled Technical Information (CTI).** A CUI category. Technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Defined in DFARS 252.204-7012(a). Includes technical data packages, drawings, specifications, process sheets, manuals, source code, and test data.
- **Export-controlled information.** Also a CUI category. ITAR technical data (22 CFR 120) and EAR technology (15 CFR 772) overlap heavily with CTI. A custody model that satisfies CTI requirements will satisfy most export-control custody expectations, and the reverse is not true.
- **Covered defense information.** The DFARS 7012 term for CUI, including CTI, that is marked or otherwise identified in the contract and provided to or generated by the contractor in performance. This is the information the clause requires you to protect, report incidents on within 72 hours, and flow down.
- **CTI at inception.** DoW Instruction 8430.01, paragraphs 3.2.f.(3), 3.5.e.(2), and 3.7.a.(b), designates software and its technical artifacts with a specific military or space application as CTI from the moment they are created, not when someone marks them. That principle should be applied to all CTI, not only software.

2.2 Where CTI actually lives

A boundary that stops at the file server and the email tenant is the most common scoping failure in the DIB. CTI in a typical small or mid-size contractor lives in at least five environments, and the F-35 diversion is a reminder that the last two are the ones most often left out.

Environment	Typical CTI	Why it gets missed
Engineering and design	Technical data packages, CAD models, drawings, specifications, analysis results	Usually in scope, but PLM systems, engineering workstations, and personal drives of engineers often are not
Manufacturing and repair	Process sheets, work instructions, inspection records, NC programs, repair procedures	Treated as operations rather than information; shop floor systems and OT rarely appear on boundary diagrams
Software development	Source code, build scripts, SBOMs, test vectors, design documents, CI/CD pipeline configuration	Developers use cloud repositories and AI tools outside IT's view; 8430.01 makes all of it CTI at inception
Logistics and shipping	Manifests, routing instructions, packing lists, customs documents, chain-of-custody forms	Handled by freight forwarders and 3PLs; contractors assume the carrier's system is the carrier's problem
Third parties	Anything above, held by subcontractors, repair partners, contract developers, intermediaries	Flow-down clauses exist on paper; nobody verifies the third party's boundary or custody records

The F-35 canopy was in the fourth and fifth environments when it went missing. A contractor whose boundary diagram does not include its shipping systems and its intermediaries has the same blind spot.

3. The Regulatory State as of September 2026

There is a great deal of noise in the market about what is and is not required. The table below is the position as of this paper's date. Items marked with an asterisk are expected to change when the CMMC Reform Task Force reports.

Instrument	Status	What it requires of a contractor holding CTI
DFARS 252.204-7012	In force, unchanged	Adequate security per NIST SP 800-171; 72-hour cyber incident reporting to DIBNet; media preservation; flow-down to subcontractors under paragraph (m)
NIST SP 800-171 Rev 2	Contractual baseline	110 requirements. Rev 2 remains the assessed version under DoW class deviation; Rev 3 adoption into the DFARS is pending
DFARS 252.204-7019 /	In force	Current SPRS score and assessment date; DoW right to

Instrument	Status	What it requires of a contractor holding CTI
7020		conduct Medium or High assessments (DIBCAC)
CMMC Phase 1 (32 CFR 170)	In force since Nov 10, 2025	Level 1 or Level 2 self-assessment and annual affirmation as a condition of award where the contract requires it
CMMC Phase 2 *	Suspended Jul 13, 2026; codified by Class Deviation 2026-O0025 Rev 3, Sep 3, 2026	Third-party (C3PAO) assessment requirements removed from contracts; no replacement date
CMMC Reform Task Force *	Review closed ~Sep 11, 2026; report pending	Recommendations on scalability and cost; the underlying CUI protection obligation is not under review
False Claims Act	Active enforcement	Inaccurate affirmations and SPRS scores are actionable; Aerojet Rocketdyne (2022, $9M) and Honeywell Aerospace (2026, $2M) are the reference cases
DoW Instruction 8430.01	Effective Sep 8, 2026	Binds DoW Components; reaches contractors through contract clauses: CTI at inception for software artifacts, pipelines as critical infrastructure, machine-readable evidence, government access to contractor and subcontractor metrics
ITAR (22 CFR 120 to 130)	In force	Defense articles and technical data; Hong Kong treated as China since 2020; freight forwarder and intermediary obligations
FAR CUI rule *	Proposed	Would extend standardized CUI handling and 800-171 expectations government-wide; not final

The honest summary: the third-party certification gate is on hold, and every underlying obligation is intact and being enforced. A contractor that read the July suspension as permission to slow down misread it.

4. From Records the Government Must Ask For to Evidence It Can Pull

The department's response to its visibility problem is written most clearly in DoW Instruction 8430.01. Although the instruction is scoped to software, the principles it establishes are the ones a contractor should expect to see in every future instrument.

- **Paragraph 3.5.a:** All software operated on DoW networks will be supported by machine-readable evidence of its component composition, build integrity, and application security. Evidence is a condition of operation, not a response to a request.

- **Paragraph 3.5.c:** Covered software will be produced through a secure, automated, observable build process that generates provenance and cryptographically verifiable attestations of pedigree, a chain of custody for the software and its components.
- **Paragraph 3.3.d.(1):** Contracts will specify government rights to access metrics and supporting data from contractor and subcontractor environments. Visibility is written into the contract, not negotiated after an incident.
- **Paragraph 3.4.d:** Authorizing officials will accept standard machine-readable evidence to grant reciprocity. Evidence in the right form replaces redundant assessment; evidence in the wrong form does not count.
- **Paragraph 3.5.h.(2):** Vendors must report critical or actively exploited vulnerabilities within a CIO-specified timeframe as a condition of deployment or continued use.

Put the GAO finding beside these paragraphs and the logic is explicit. Contractor-controlled records that the government has to ask for are the model that failed. Evidence the government can verify on its own is the replacement. The CMMC affirmation, the SPRS score, and the DIBCAC assessment are earlier versions of the same idea. 8430.01 is the first instrument to state it as a design principle.

> **Implication for custody**
>
> Custody evidence that exists only as a narrative in an SSP, or as records a contractor would have to assemble on request, will increasingly be treated as no evidence at all. The standard is a record that exists before anyone asks and that a third party can read without the contractor explaining it.

5. A Custody Model: Know, Locate, Prove, Flow

The model below organizes CTI custody into four questions. Each question maps to one phase of the Cyber G.A.R.D. Framework, to the NIST SP 800-171 requirements that make it a contractual obligation, and to the evidence that demonstrates it. The phases are sequential for a reason. A scoping error in the first phase invalidates everything after it, which is precisely what the F-35 program is now demonstrating.

Question	Cyber G.A.R.D. phase	Primary 800-171 families and clauses	Evidence that satisfies it
Know: what CTI do we hold and where may it exist?	Govern the boundary	3.1 Access Control; 3.4 Configuration Management (3.4.1 baselines, 3.4.2 inventory); 32 CFR 170.19 asset categories	CTI inventory by asset class; boundary diagram covering all five environments; data flow diagram; third-party register
Locate: where is each item right now?	Align evidence	3.8 Media Protection (3.8.1 to 3.8.9); 3.10 Physical Protection; 3.13 System and Communications Protection	Marking at inception; asset tags and media logs; shipment and transfer records; location field in the inventory that is current, not historical

Question	Cyber G.A.R.D. phase	Primary 800-171 families and clauses	Evidence that satisfies it
Prove: who has touched it and when?	Reinforce implementation	3.3 Audit and Accountability (3.3.1, 3.3.2, 3.3.5); 3.1.1, 3.1.2; 3.8.5 (control access to media during transport)	Audit logs retained and reviewed; chain-of-custody records for physical and digital transfers; access reviews; incident reports within 72 hours under 7012(c)
Flow: do our obligations reach every party that holds it?	Defend the assessment	DFARS 7012(m); ITAR intermediary and freight forwarder provisions; 800-171 Rev 3 Supply Chain Risk Management family (03.17) when adopted	Executed flow-downs; third-party attestations or assessments; intermediary contracts with custody and reporting terms; evidence the third party's boundary was reviewed

5.1 Govern: build the inventory before anything else

The inventory is the foundation. It must be organized by the CMMC asset categories in 32 CFR 170.19 because that is how an assessor will read it: CUI assets, security protection assets, contractor risk managed assets, specialized assets, and out-of-scope assets. For each CTI asset the record needs an owner, a location, a classification (CTI, export-controlled, both), a custodian, and a source contract.

Practical requirements that most programs miss:

- Include software repositories, build servers, CI/CD runners, artifact registries, and any AI coding assistant developers use. Under 8430.01 these are CTI-handling assets and, for pipelines, critical infrastructure.
- Include shipping and logistics systems, whether yours or a carrier's, and the intermediaries themselves as third-party assets.
- Include repair partners and the systems they use to receive your procedures and return your data.
- Record where CTI is permitted to exist, not only where it is. A location that is not on the permitted list is a finding when CTI is found there.

The Govern phase ends with a boundary the contractor can defend, and a written rationale for every asset excluded from it.

5.2 Align: mark at inception and keep the location field current

Custody fails at the moment CTI is created and not marked, because unmarked information moves without triggering any control. 8430.01's rule for software, CTI at inception, is the right rule for everything. Engineering templates, repair procedure templates, and shipping document templates should carry the CUI designation indicator and the CTI category marking from the first save.

For physical media and shipments, NIST SP 800-171 requirements 3.8.1 through 3.8.9 supply the controls: protect and limit access to media, mark media with distribution limitations, control access during transport, and account for media during transport outside controlled areas. The evidence is a media log or shipment record that shows the item, the marking, the custodian, the destination, and the hand-off. The F-35 shipment lacked a control that would have flagged a Pacific crossing ending in the wrong port; a shipment record with an expected route and a required receipt confirmation is that control.

The inventory's location field must be current. An inventory that records where an item was when the inventory was built is a history, not a custody record.

5.3 Reinforce: make custody records exist before anyone asks

The Prove question is answered by records that are generated as a by-product of work, not assembled afterward. Three mechanisms carry most of the load:

1. Audit logging under 3.3.1 and 3.3.2, retained long enough to cover an assessment cycle and reviewed under 3.3.5 so that anomalies are found by the contractor rather than by an assessor or a reporter.
2. Chain-of-custody records for every transfer of CTI across a boundary: to a subcontractor, to a repair partner, to a carrier, to a cloud service, or into a build pipeline. The record identifies what moved, who authorized it, who received it, and when receipt was confirmed.
3. Incident and anomaly reporting on a fixed clock. DFARS 7012(c) requires reporting cyber incidents to DIBNet within 72 hours of discovery. 8430.01 paragraph 3.5.h.(2) adds a CIO-specified window for critical vulnerabilities. A shipment that misses its expected receipt window should trigger the same discipline internally.

This phase is also where AI-assisted development must be brought under control. 8430.01 paragraph 3.6.b prohibits entering non-public DoW information into generative AI services that are not hosted on DoW systems and approved. A contractor whose developers paste CTI into a consumer AI tool has lost custody of it. Policy, an approved-tool list, and review gates for AI-generated changes to security-critical code (paragraph 3.6.a) are the reinforcement.

5.4 Defend: extend custody through flow-down and keep the proof current

The Flow question is where the F-35 diversion happened. Custody that ends at the contractor's own walls is not custody. DFARS 7012(m) requires the clause to be flowed to subcontractors whose performance involves covered defense information, and the flow-down is only the first step. The contractor has to verify that the subcontractor, repair partner, contract developer, or intermediary can answer the same four questions, and has to retain evidence of that verification.

For intermediaries and freight forwarders the requirements are contractual: expected routing, prohibited transit points, custody confirmation at each hand-off, notification within a fixed window when a shipment deviates, and the right to audit records. ITAR imposes its own obligations on forwarders handling defense articles; a contractor should not assume the forwarder's compliance program covers the contractor's exposure.

Defend also means keeping the evidence current for the parties who will test it. The annual CMMC affirmation and the SPRS score are attestations under the False Claims Act; an inventory and custody record that support them are the defense. When the Reform Task Force reports and third-party assessment returns in whatever form, the contractor with an inventory, current locations, chain-of-custody records, and verified flow-downs will have nothing to reconstruct.

6. A Ninety-Day Roadmap

The model above can be implemented by a small contractor in one quarter without waiting for any rule. The sequence matters; do not start at day 61.

Days 1 to 30: Govern

- Identify every contract that provides or generates CTI and the clauses it carries (7012, 7019, 7020, 7021, ITAR).
- Build the CTI inventory by asset category across all five environments, including software pipelines, logistics, and third parties.
- Draw the boundary and the data flows; write the exclusion rationale for every asset left out.
- Update the SSP scoping section to match. If the boundary changed, the SPRS score probably will too; recalculate it.

Days 31 to 60: Align and Reinforce

- Apply CUI and CTI markings to templates so new information is marked at inception; remediate the highest-value existing unmarked CTI.
- Stand up media, shipment, and transfer logs with required receipt confirmation and expected routing.
- Confirm audit logging covers every CTI-handling system, including repositories and build servers, and that someone reviews it on a schedule.
- Publish the AI-assisted development policy and approved-tool list; close consumer AI tools to CTI.

Days 61 to 90: Defend

- Execute or re-execute 7012 flow-downs and custody terms with every third party in the inventory, including intermediaries and forwarders.
- Obtain a written attestation or a boundary review from each third party; record the result.
- Run the self-check in Appendix A as a mock assessment; convert every gap into a POA&M item with an owner and a date.
- Re-affirm in SPRS only when the inventory, the custody records, and the flow-downs support the score.

7. What to Expect Next

Four developments will change the detail of this paper without changing its direction.

- **The CMMC Reform Task Force report.** Expected in late September or early October 2026. Its stated concerns are assessor capacity and cost. Whatever it recommends for the assessment gate, it is not expected to relax the underlying CUI protection obligation, and it may lean harder on DIBCAC assessments, SPRS accuracy, and FCA enforcement in the interim.
- **NIST SP 800-171 Rev 3 adoption.** Rev 3 adds a Supply Chain Risk Management family (03.17) and strengthens several custody-relevant requirements. The DoW has kept Rev 2 as the contractual baseline by class deviation; when Rev 3 enters the DFARS, the Flow question becomes an explicit requirement family.
- **8430.01 flow-down.** The instruction reaches contractors through contract language. Expect CTI-at-inception, evidence-package, and vulnerability-reporting terms in solicitations and prime flow-downs for software-intensive work well before any DFARS change.
- **The FAR CUI rule.** If finalized, it extends standardized CUI handling and 800-171 expectations to civilian agencies. Contractors serving both DoW and civilian customers should build one custody model, not two.

Conclusion

The department did not lose a million F-35 parts because its contractors were careless. It lost them because it could not see what its contractors held, and the records that would have told it were not its own. The F-35 diversion is the same failure with a foreign jurisdiction attached. DoW Instruction 8430.01 is the department's statement that it will not accept that condition for software, and the pattern of enforcement during the CMMC pause is its statement that the obligation to protect CUI does not move when an assessment date does.

A contractor that can answer the four custody questions with evidence is protected on every front at once: against the assessor, against the prime, against the False Claims Act, and against the reporter. A contractor that cannot is one diverted shipment away from being the story.

> **How Globe-America Consulting can help**
>
> Our advisory engagements implement this model through the Cyber G.A.R.D. Framework: boundary and inventory work in Govern, marking and custody records in Align, logging and AI-development policy in Reinforce, and flow-down verification and assessment readiness in Defend. Every engagement begins with a readiness consultation. Contact eddie.white@globe-america.com or visit globe-america.com.

Appendix A: CTI Custody Self-Check

Answer each item Yes, Partial, or No. Any answer other than Yes is a POA&M item. The check is designed to be run in an afternoon by the person who owns the SSP.

#	Question	Phase	Answer
1	We have a written inventory of CTI organized by CMMC asset category, with an owner, custodian, location, and source contract for each item.	Govern	
2	The inventory includes software repositories, build servers, CI/CD runners, artifact registries, and AI tools used by developers.	Govern	
3	The inventory includes shipping and logistics systems and names every intermediary, carrier, and repair partner that handles CTI.	Govern	
4	The boundary diagram and data flow diagram match the inventory, and every excluded asset has a written rationale.	Govern	
5	Templates for engineering, manufacturing, software, and shipping documents carry CUI and CTI markings so new information is marked at inception.	Align	
6	The location field in the inventory reflects where each item is now, and it has been verified within the last quarter.	Align	
7	Every shipment or transfer of CTI has a record with expected routing, custodian, destination, and required receipt confirmation.	Align	
8	Audit logs cover every CTI-handling system, are retained across an assessment cycle, and are reviewed on a schedule by a named person.	Reinforce	
9	Chain-of-custody records exist for transfers to subcontractors, repair partners, carriers, cloud services, and build pipelines.	Reinforce	
10	A written policy names the AI tools approved for development, prohibits CTI in consumer AI services, and requires human review of AI-generated changes to security-critical code.	Reinforce	
11	A cyber incident or a missed shipment receipt triggers a documented process with a fixed reporting clock (72 hours to DIBNet for cyber incidents).	Reinforce	
12	DFARS 7012 has been flowed down to every third party in the inventory, and we hold the executed documents.	Defend	
13	Intermediary and forwarder contracts specify routing, prohibited transit points, hand-off confirmation, deviation notification, and audit rights.	Defend	
14	We hold a current attestation or boundary review from each third party that handles CTI.	Defend	
15	Our SPRS score and CMMC affirmation are supported by the inventory, custody records, and flow-down evidence, and we could produce that	Defend	

#	Question	Phase	Answer
	evidence within one business day.		

References

Government Accountability Office. F-35 Program: DOD Needs Better Accountability for Global Spare Parts and Reporting of Losses Worth Millions. GAO-23-106098, May 23, 2023.

Politico. Reporting on the diversion of F-35 components to Hong Kong and associated congressional briefings, September 18, 2026. Related coverage: FreightWaves; Defence Security Asia; F-35 Joint Program Office statement.

Department of War. DoW Instruction 8430.01, Accelerated Mission Software. Office of the DoW Chief Information Officer, effective September 8, 2026.

Department of War. Class Deviation 2026-O0025, Revision 3, September 3, 2026 (CMMC Phase 2 suspension).

Department of Justice. Settlement with Honeywell Aerospace resolving False Claims Act allegations concerning NIST SP 800-171 compliance, September 1, 2026.

Department of Justice. Settlement with Aerojet Rocketdyne resolving False Claims Act allegations concerning cybersecurity requirements, July 2022.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; DFARS 252.204-7019, 7020, 7021, 7025.

32 CFR Part 170, Cybersecurity Maturity Model Certification Program; 32 CFR 170.19, CMMC scoping and asset categories.

32 CFR Part 2002, Controlled Unclassified Information; DoD Instruction 5200.48, Controlled Unclassified Information (CUI), March 6, 2020.

National Institute of Standards and Technology. SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations; SP 800-171 Revision 3, May 2024.

22 CFR Parts 120 to 130, International Traffic in Arms Regulations; Executive Order 13936, The President's Executive Order on Hong Kong Normalization, July 14, 2020.

Globe-America Consulting. The Cyber G.A.R.D. Framework: Govern the boundary, Align evidence, Reinforce implementation, Defend the assessment. Framework white paper, 2026.

About the author. Eddie White is the founder and principal consultant of Globe-America Consulting, Inc., a Service-Disabled Veteran-Owned Small Business in Fort Worth, Texas. He is a CMMC Registered Practitioner, ISO 9001 Lead Auditor, and Lean Six Sigma Master Black Belt, retired from the U.S. Air Force after 20 years in civil engineering and program management, and hosts the Cyber-Brief podcast.