CUI / CTI PROTECTION · SEPTEMBER 2026

A Canopy Went to Hong Kong.

That Is Not the Part That Should Worry the Defense Industrial Base.

What the F-35 shipment diversion says about the state of CUI and CTI protection in September 2026, and why the Department of War is done taking anyone's word for it.

Eddie White

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

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

CUI / CTI PROTECTION

A Canopy Went to Hong Kong. That Is Not the Part That Should Worry the Defense Industrial Base.

What the F-35 shipment diversion says about the state of CUI and CTI protection in September 2026, and why the Department of War is done taking anyone's word for it.

By Eddie White CMMC Registered Practitioner · Founder, Globe-America Consulting · September 19, 2026

Sometime this summer, a shipment of unserviceable F-35 Lightning II components left Australia bound for the United States for repair. It never arrived. According to Politico, which broke the story on September 18, the shipment was rerouted while crossing the Pacific and ended up in Hong Kong. An intermediary was moving the parts on behalf of Lockheed Martin. Among them was reportedly a cockpit canopy, a component that incorporates low-observable technology restricted to the United States and program partners.

The F-35 Joint Program Office confirmed it is aware of what it called a shipment issue and said it is working with U.S. authorities and industry partners to recover the components, investigate the incident, and put safeguards in place. State Department and Pentagon officials began briefing congressional national security committees as early as June. As of this writing, nobody has publicly said why the shipment was diverted, whether it was a mistake or an unauthorized act, or who has the parts now.

That last sentence is the story. Not the canopy. Not Hong Kong. The fact that, weeks after the diversion, the department cannot tell Congress with confidence where a low-observable component is.

The accountability gap was already on the record

This is not the first time the F-35 program has been unable to account for its own parts. A 2023 Government Accountability Office report found that more than one million F-35 spare parts had gone missing over the preceding five years, and that the department could not review losses worth tens of millions of dollars because the prime contractor controlled the records. The government did not have the data. The contractor did.

Read that finding next to this week's news and the pattern is hard to miss. When custody of a sensitive asset passes through a chain of contractors and intermediaries, and the only record of that custody lives in contractor systems the government cannot query, the department finds out something is wrong when a foreign jurisdiction is involved and a reporter calls. That is not an espionage problem. It is a visibility problem, and visibility problems become espionage problems.

Why this is a CUI and CTI story

A canopy is hardware, so it is fair to ask what a physical logistics failure has to do with Controlled Unclassified Information. The answer is that everything wrapped around that canopy is information the government controls. The technical data package that describes it. The repair procedures the Australian depot follows. The shipping manifests, routing instructions, and chain-of-custody records that should have flagged a Pacific crossing ending in the wrong port. Under DoDI 5200.48 and DFARS 252.204-7012, technical information with a military or space application is Controlled Technical Information from the moment it exists, and the systems that process it are covered contractor information systems.

The diversion is also an export-control matter, since F-35 components are defense articles under ITAR and Hong Kong has been treated as China for export purposes since 2020; that question belongs to the State Department and the parties involved, and this piece leaves it there. Export-controlled information is itself a category of CUI, so the custody problem described here is the same problem viewed from the other side.

Physical custody and information custody are the same control problem. Both come down to three questions: Do you know what you have? Do you know where it is? Can you prove who touched it? A contractor that cannot answer those questions for a shipping container is unlikely to answer them for a file share, a repair database, or a build pipeline. The F-35 diversion is a case study in what happens when the answer to all three is a shrug.

Where CUI and CTI protection actually stands right now

It is worth being precise about the current state of play, because there is a lot of noise in the market about what is and is not required.

- DFARS 252.204-7012 and NIST SP 800-171 have not paused. They are in every applicable contract, and the 110 requirements, the SPRS score, and the annual affirmation are all live obligations today.
- CMMC Phase 1 has been in force since November 10, 2025. Level 1 and Level 2 self-assessments remain a condition of award where the contract calls for them.
- CMMC Phase 2, the transition to third-party assessment, was suspended on July 13, 2026 while a CMMC Reform Task Force reviews the program. On September 3, a class deviation made that suspension binding on contracting officers and directed them to strip third-party assessment requirements from contracts. No replacement date exists.
- Enforcement did not wait for the review. On September 1, 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. The conduct predates any CMMC clause. The government enforced through DFARS 7012 and the FCA, which have been there the whole time.
- The Reform Task Force report is expected in late September or early October. Its stated concerns are assessor capacity and cost burden on small firms, not whether CUI needs protecting.

So the honest summary is this: 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 stop was reading it wrong, and Honeywell's settlement arrived seven weeks later to make the point.

The department's answer is evidence, not trust

Ten days before the F-35 story broke, the DoW Chief Information Officer signed DoW Instruction 8430.01, Accelerated Mission Software. Most of the DIB has not read it because it is written for program offices. It should be read anyway, because it tells you where the department's thinking is headed.

Paragraph 3.5.e.(2) says that software and its technical artifacts with a specific military or space application, including source code, build scripts, SBOMs, test vectors, and design documents, are CTI at inception and must be protected at moderate confidentiality and integrity. Paragraph 2.8.b says CI/CD pipelines are critical infrastructure that must be authorized, monitored, and protected. Paragraph 3.5.a says all software operated on DoW networks will be supported by machine-readable evidence of its composition, build integrity, and application security. Paragraph 3.3.d writes government access to metrics and supporting data from contractor and subcontractor environments directly into contracts.

Put the GAO finding, the F-35 diversion, and 8430.01 in a row and the direction is unmistakable. The department spent years discovering it could not see what its contractors held. It is now writing policy that says it will not accept that condition for software, and it is doing so by demanding proof in a form it can verify itself. Contractor-controlled records that the government has to ask for are exactly the model that failed. Machine-readable evidence the government can pull is the replacement.

That shift will not stay confined to software. The same logic that produced 8430.01 will show up in whatever the Reform Task Force recommends, in the next revision of DFARS 7012, and in prime flow-downs long before any of it becomes a rule.

Five questions to ask your own program this week

None of this requires waiting on the task force. A contractor handling CTI in any form can test itself against the standard the F-35 program just failed.

- Inventory. Can you name every system, location, and third party that holds CTI, including development environments, repair and logistics systems, and the intermediaries you pay to move things? If your boundary diagram stops at the file server, it is incomplete.
- Custody. For any CTI asset, physical or digital, can you produce a record of where it is and who has handled it without reconstructing it from email?
- Flow-down. Do your DFARS 7012 and NIST SP 800-171 obligations reach the freight forwarder, the repair partner, and the contract developer, or do they stop at your own walls? The F-35 canopy was in an intermediary's hands when it went missing.
- Marking. Is CTI identified and marked when it is created, or when someone gets around to it? 8430.01 says at inception. Your policy should say the same.
- Proof. If a contracting officer, a DIBCAC assessor, or a prime asked you tomorrow to demonstrate all of the above, could you show evidence, or would you be asking them to take your word for it?

These are the questions the Cyber G.A.R.D. Framework is built around: govern the boundary before anything else, align the evidence to it, reinforce the implementation, and defend the result when someone comes to check. The order matters. A scoping mistake at the first step invalidates everything after it, which is the lesson a canopy in Hong Kong is teaching the F-35 program right now.

The bottom line

The suspension of CMMC Phase 2 changed the date of one assessment. It did not change the obligation, it did not change enforcement, and it did not change the department's loss of patience with contractors it cannot see into. The F-35 diversion is a reminder of what that blindness costs. DoW Instruction 8430.01 is a preview of what the department intends to do about it. Contractors who close the visibility gap on their own terms now will be in a far better position than those who wait for a rule, a prime, or a reporter to do it for them.

Sources

Politico, September 18, 2026, reporting on the F-35 shipment diversion and congressional briefings; F-35 Joint Program Office statement as reported by FreightWaves and Defence Security Asia; Government Accountability Office, 2023 report on F-35 spare parts accountability; Department of War Class Deviation 2026-O0025, Revision 3, September 3, 2026; Department of Justice settlement announcement, Honeywell Aerospace, September 1, 2026; DoW Instruction 8430.01, Accelerated Mission Software, effective September 8, 2026; DoDI 5200.48; DFARS 252.204-7012; 32 CFR Part 170; 22 CFR Parts 120 to 130 (ITAR); Executive Order 13936 on Hong Kong normalization.

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