Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/dfars-cmmc-draft-has-been-released/

DEFENSE CONTRACTOR COMPLIANCE

DFARS 252.204-7012 and CMMC 2.0 Readiness, Penetration Testing and Incident Reporting for Defense Contractors

A defense contractor that discovers an intrusion inherits a 72 hour report to the Department of Defense and a 90 day duty to preserve images and packet data. Image the affected systems first, rebuild afterward and bring counsel and an examiner in now. Call (800) 868-8189 at any hour.

Published September 12, 2019 · Updated October 30, 2026

Primary Reference for This Guide

Start with DoD CIO overview of the CMMC program.

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

From Self Attestation to CMMC 2.0 and False Claims Scrutiny

For defense contractors, aerospace manufacturers and subcontractors handling Federal Contract Information or Controlled Unclassified Information, the era of informal self attestation is over. With CMMC 2.0 aligned directly to NIST SP 800-171 controls and active Department of Justice Civil Cyber Fraud Initiative enforcement under the False Claims Act, inaccurate system security plans or unverified security controls carry severe financial and contractual penalties. Equally critical, DFARS clause 252.204-7012 requires contractors discovering a cyber incident to report it to the Department of Defense within seventy two hours and preserve images of all known affected information systems and relevant monitoring packet data for at least ninety days.

Reading 252.204-7012 as an Examiner Reads It

The clause is short and its obligations are specific. Paragraph (c) requires a contractor that discovers a cyber incident affecting a covered contractor information system to review for evidence of compromise and to report rapidly through the DIBNet portal, and the clause defines rapid reporting as within 72 hours of discovery. Paragraph (e) is the one examiners live with: the contractor "shall preserve and protect images of all known affected information systems" and all relevant monitoring and packet capture data for at least 90 days from the report, so that the Department can request the media or decline interest. The full text is on acquisition.gov. Read those two paragraphs together and the engagement writes itself: identify the affected systems quickly, image them before anyone remediates, and keep the images and captures for the required window.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The word known carries the most weight. Affected systems are identified in the review the clause requires, and that review often widens as analysis proceeds, which means the preservation duty attaches to systems discovered on day ten as well as day one. We treat every host that touched the adversary's path, every identity used and every network segment that carried the traffic as presumptively in scope until the record rules it out. The clause also flows down to subcontractors handling covered defense information, so a prime's exposure includes how its suppliers handled those first hours. Our DFARS compliance page sets out how we help contractors stand up that review and preservation workflow before a report is ever needed, and why doing so protects the contract and the people who certify under it.

The CMMC Cadence a Contractor Lives By

CMMC 2.0 turns the NIST SP 800-171 requirements into a certification calendar. Level 1 covers Federal Contract Information with an annual self assessment and affirmation. Level 2 maps to the full set of SP 800-171 requirements for Controlled Unclassified Information, with some contracts allowing a self assessment and others requiring an assessment by an authorized third party assessment organization on a three year cycle, backed by an annual affirmation from a senior official. Level 3 adds requirements drawn from NIST SP 800-172 and is assessed by the government. The Department publishes the program structure and rulemaking status at dodcio.defense.gov/CMMC, and Level 2 assesses the requirements of SP 800-171 Revision 2, the revision 32 CFR 170.2 incorporates, even though NIST has since published Revision 3. On July 13, 2026 the Department of War Chief Information Officer suspended the November 2026 Phase 2 transition, and Class Deviation 2026-O0025 Revision 3 carries that direction into solicitations and contracts. The affirmation is where False Claims Act exposure sits, because a senior official signs a statement the government may later test against the system as it actually ran.

The cadence inside that calendar is what keeps a certification honest. Scores posted to the Supplier Performance Risk System must reflect the current state of the system, plans of action and milestones have a closeout window the rule fixes rather than an open ended promise, and any significant change to the CUI enclave reopens the question of whether the system security plan still describes reality. We recommend a quarterly review of the plan against configuration exports, an annual manual penetration test of the enclave boundary, and a tabletop exercise that walks the incident reporting path end to end. Those cycles produce dated evidence of diligence, which is the record a contractor wants in hand when a prime, an assessor or a Department of Justice attorney asks what was true on a particular date. Our penetration testing page explains how an enclave test is scoped.

What the Logs Can Establish About CUI Exposure

The audit and accountability family in SP 800-171 exists so that, after an incident, someone can reconstruct who did what to covered information. When those controls are real, the record is rich: authentication logs showing the account and source, endpoint telemetry showing process execution and file access, firewall and proxy logs showing egress volume and destination, and NetFlow or packet captures showing what left and when. Correlated, those sources let us bound which CUI files were opened or staged, whether a compression and transfer tool such as rclone or an archive utility ran, and how much data crossed the boundary. That bounding is what the DIBNet report, the prime notification and the customer conversation all depend on.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Where logging was lighter, the report states plainly which sources were available and works from them. For a period with no egress log, the report says which records cover it and what they show, the kind of candor that keeps the government's confidence in the whole report. We look for the adversary's path, the accounts used, the dwell time and the systems touched in artifacts that commonly persist even on lightly logged networks: Windows event logs, registry and prefetch evidence, shadow copy remnants, mail server logs and the cloud tenant audit trail. The logging picture itself becomes a finding, because it tells the contractor which SP 800-171 requirement to strengthen before the next affirmation. Our data breach analysis page describes how the scope question is worked for regulated data.

Running a DFARS Incident Engagement Phase by Phase

The first phase is triage under counsel, and it runs in hours. We confirm what was observed, identify the systems and identities believed affected, and establish a preservation plan that images those systems before any remediation, because imaging comes first and rebuilding follows. Volatile data comes first: memory, running processes, network connections and the logs that roll fastest. Full disk images follow, hashed and documented, along with exports of firewall, proxy and authentication logs and any packet capture the contractor holds. Doing this alongside containment keeps recovery moving and lets the contractor meet the 90 day preservation duty and show the Department that the evidence was handled with care from the start.

Scoping and analysis form the second phase, and they feed the report rather than following it. Within the 72 hour window the contractor needs enough facts to file a credible initial report, knowing that supplemental reports are expected as analysis matures. We work the timeline, the lateral movement, the data staging and the egress to answer the questions the report form asks and the questions the prime will ask next. The third phase produces the written record: a chronology, the affected system list, the CUI exposure assessment with its basis and scope, and the remediation facts the system security plan will need to reflect. Our defense contractor records package lists what to gather so each phase starts with the material in hand. A contractor that follows this path protects the contract, the affirmation and the executives who signed it.

Practices That Turn an Incident Into a Documented Event

The most valuable practice is imaging first. An IT team under pressure to get production back images the affected servers before wiping and reimaging them, so the images the clause requires exist from the first day. The second is keeping the system security plan a description of the system as it runs, so the affirmation describes the controls actually enforced. The third is filing a report whose certainty matches the record, stating what the collected logs show about CUI access and what analysis continues. These practices matter on the legal side as much as on the engineering side, because the government and a relator's counsel read the record as evidence of what the contractor knew and chose to say.

Each practice is procedural. Write the preservation step into the incident response plan ahead of containment so the order of operations is settled before the incident. Keep configuration exports and control test results dated alongside the system security plan so the affirmation rests on evidence rather than belief. Draft the DIBNet report with counsel and the examiner together so every factual statement traces to an artifact, and use the supplemental report mechanism when the record changes, so each statement keeps pace with the

© 2026 Global Digital Forensics, Inc. All rights reserved.

evidence. A standing incident response retainer settles the contract terms, contact tree and network familiarity in advance, which is what makes a 72 hour clock achievable. Contractors who prepare this way turn an incident into a documented event.

From Incident Report to Declaration When the Government Asks Questions

The same record that supports the DIBNet report may later support a declaration in a contract dispute, a response to a Department of Justice civil inquiry, or testimony in a False Claims Act matter. We write for that possibility from the first day. Each finding in our report names the artifact behind it, the tool and version used, the hash of the image it came from and the reach of the inference, so that a statement made in week one can be sworn to in year two without revision. Where a control was not operating, the report records it accurately, because an accurate account is the one a contractor can defend over time.

Our examiners have testified in federal and state courts and our work has been accepted by courts, and that experience shapes how a defense contractor report is built. Counsel receives a document that distinguishes observation from inference, a chronology that can be walked under cross examination, and an examiner who can explain the NIST control families in terms a judge or a Department official can follow. Our government sector page describes the contracting environments we support, and our expert witness services page explains how a report moves to deposition and trial. Preparing the record to that standard protects the contractor on the day of the incident and on the day, often years later, when someone asks what the company knew.

How Global Digital Forensics Supports Defense Industrial Base Contractors

Global Digital Forensics has supported counsel and their clients since 1992 across both proactive compliance and emergency incident response, and defense contractors bring us both kinds of work. Ahead of CMMC assessments, our engineers validate your NIST SP 800-171 controls, conduct manual penetration testing across CUI enclaves and remediate architectural gaps. If a suspected intrusion occurs, our forensic examiners deploy immediately under the direction of your legal counsel to execute DFARS compliant forensic imaging and ninety day packet preservation while working the scope of CUI exposure within the seventy two hour reporting window. Our defense contractor records package lists what to gather before an assessment or an incident report. Call (800) 868-8189 to speak with our DFARS and CMMC specialists. The initial consultation is free.

The CMMC Levels and the DFARS Clock for Contractors

The guide reads DFARS 252.204-7012 the way an examiner does and sets out the CMMC certification cadence. This table states each level and obligation, what it covers and the assessment or deadline attached, so a contractor can see where False Claims Act exposure sits and when the clocks run. Read the DFARS rows as the duties that attach at discovery of an incident. The affirmation is a statement a senior official signs that the government may later test against the system as it actually ran.

© 2026 Global Digital Forensics, Inc. All rights reserved.

CMMC levels and DFARS 252.204-7012 duties, what each covers and the assessment or deadline attached.

Obligation	What it covers	Assessment or deadline
CMMC Level 1	Federal Contract Information	Annual self assessment and affirmation
CMMC Level 2	Controlled Unclassified Information under SP 800-171	Self or third party assessment on a three year cycle
CMMC Level 3	Requirements drawn from SP 800-172	Assessed by the government
DFARS rapid reporting	A cyber incident on a covered system	Within 72 hours through the DIBNet portal
DFARS media preservation	Images of affected systems and packet data	At least 90 days from the report
Supplier flowdown	Subcontractors handling covered defense information	The clause flows down to them
Senior official affirmation	The system as it actually ran	Annual, and where False Claims Act exposure sits

How to Begin and What Happens on the First Call

Bring the contract numbers and clauses in play, a diagram or description of the CUI enclave, the system security plan, what was observed and when, and a list of any containment or rebuild steps already taken. The examiner asks which systems and accounts are believed affected, whether images and packet captures exist, how authentication and egress are logged, who the prime and contracting officer contacts are, and when discovery occurred for purposes of the 72 hour clock. Counsel then receives a written scope covering preservation, analysis and report support, a timing estimate tied to the reporting deadline, and a written proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers at any hour.

Sources and Related Reading

Authorities cited in this guide: DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Establishes the 72 hour rapid reporting definition, the review for evidence of compromise and the 90 day preservation of images and packet data, clause text as currently published on acquisition.gov. DoD CIO, Cybersecurity Maturity Model Certification. Establishes the CMMC 2.0 level structure, assessment types and rulemaking status, official program page as of October 2026. NIST SP 800-171 Revision 2. Sets the security requirements for Controlled Unclassified Information that a CMMC Level 2 assessment tests, the revision incorporated by reference in 32 CFR 170.2.

© 2026 Global Digital Forensics, Inc. All rights reserved.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About Defense Contractor Compliance

What does DFARS 252.204-7012 require after a cyber incident?

The clause requires a contractor that discovers a cyber incident affecting a covered contractor information system to review for evidence of compromise, report to the Department of Defense through DIBNet within 72 hours of discovery, and preserve images of all known affected systems and relevant monitoring and packet capture data for at least 90 days from the report. It also requires submitting isolated malicious software to the designated DoD center and cooperating with any damage assessment. We help counsel run the review and preservation so the report rests on facts.

Does a CMMC Level 2 certification require a third party assessment?

It depends on the contract. The program allows a self assessment for some Level 2 contracts and requires an assessment by an authorized third party assessment organization for others, with an annual affirmation by a senior official in both cases. The Department's CMMC site sets out which applies and how the phased rollout works. Our role is technical: we test the enclave, validate the controls against the system as it actually runs, and document the evidence an assessor or affirming official will rely on.

How long does a DFARS incident forensic engagement take?

The first phase runs on the 72 hour reporting clock, so preservation and triage happen in hours. The full scope analysis depends on how many systems were touched, how well the enclave was logged, whether the adversary staged and exfiltrated data, and how fast the contractor can produce images and logs. Supplemental reports to the Department are expected as the record matures. We give counsel a phased timing estimate at the first call and update it as the affected system list settles.

What drives the cost of a CMMC readiness or penetration testing engagement?

Scope drives it: the number of systems in the CUI enclave, whether the boundary is on premises, cloud or mixed, how many of the SP 800-171 requirements need hands on validation rather than document review, and whether a manual penetration test and a retest are included. A contractor with a tight enclave and current configuration exports is a smaller engagement than one with CUI spread across general business systems. The initial consultation is free and the proposal sets a fixed scope before work begins.

Can a contractor report to DoD before the forensic analysis is finished?

Yes, and it should. The 72 hour report is an initial report based on what is known at the time, and the clause anticipates follow up reporting as analysis continues. The first report states its certainty at the level the record supports. We help counsel draft a report that states what has been observed and what remains under examination, so later supplements add detail to a position the government can rely on.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Web Addresses for the Sources Cited

1. DoD CIO overview of the CMMC program: https://dodcio.defense.gov/cmmc/About/
2. acquisition.gov: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
3. dodcio.defense.gov/CMMC: https://dodcio.defense.gov/CMMC/
4. SP 800-171 Revision 2: https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.