Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/audit-discovery-preparation/03-defense-contractor/

AUDIT AND DISCOVERY PREPARATION

Defense contractor cybersecurity information gathering package

Gather defense contract clauses, system scope and cybersecurity records for a CMMC or NIST SP 800-171 specialist. Record each open duty for the specialist.

Gather the contract, information flow and existing security records a CMMC or NIST SP 800-171 specialist needs to propose and scope work.

Contract managers, small business owners, CISOs, project coordinators and IT providers

FCI/CUI safeguarding and CMMC preparation. The package organizes the records, and scoring, status and the assessment itself rest with the required assessor.

Before you gather

Current official program announcements report the July 13 2026 suspension of the CMMC Phase II transition previously scheduled for November 2026, while Phase I and safeguarding continue. Class Deviation 2026-O0025 Revision 3 directs contracting action and retains NIST SP 800-171 Revision 2 safeguarding. Ask for the actual solicitation amendments and the signed contract modifications; the signed contract and its modifications set the client's obligations, so the contract file is the artifact the specialist reads first, with website announcements as context.

The contract administrator supplies the incorporated clauses, the dates, the prescribed assessment type and the written flowdowns. The specialist resolves conflicts among the actual contract, the current deviations and the program rules. NIST has published Revision 3 of SP 800-171 and SP 800-171A, but the CMMC rule at 32 CFR 170.2 and the 2026 implementation memo retain Revision 2 for the stated baseline, so the correct contract criterion is the revision those instruments name. Confirm the exact paired requirements and assessment methods before mapping evidence, so the evidence is mapped once, to the right revision.

FCI, CUI, export controlled information and classified information have different bases. Ask the government or customer owner about CUI categories, markings and handling, and record who confirmed each. The required level and boundary come from the contract and the customer's designations, and a defense customer, a confidential label, a CAGE code or a domestic cloud region are context the specialist reads alongside them. Keep sensitive records and assessment artifacts in the agreed controlled environment; the preparation index describes them and points to them, so CUI, security protection information and export controlled material stay inside that controlled environment.

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

Give each request to the suggested owner. Record each answer, including the items awaiting confirmation, in the editable CSV checklist. Keep the records themselves in a secure evidence location agreed with the recipient and use the checklist as the index that points to them; passwords stay with their owners, and real patient data and controlled technical information stay in the secure location.

Records to find

CSV files hold plain records, and your spreadsheet sets the layout. Import as UTF-8, keep IDs as text, wrap text and widen columns before use. Blank client fields are intentional.

CM-R01 Actual contract package

Ask
Contract administrator

Gather
Solicitation, statement of work, contract, orders, incorporated clause versions, flowdowns, amendments, modifications, options and correspondence about CMMC.

Where to ask
Contract repository and prime customer

Why it may be needed
Establishes the basis for specialist scoping.

If missing or uncertain
Ask prime/contract officer through authorized client channels; record open interpretations for the specialist.

Reference: CM04; CM05; CM06; CM07

CM04 CM05 CM06 CM07

CM-R02 Current implementation instructions

Ask
Contracts and counsel

Gather
Current applicable deviations, written direction and modification history addressing the July 2026 suspension and any subsequent changes.

Where to ask
Contract file and official deviation index

Why it may be needed
Keeps the plan on the current instrument and its dates.

If missing or uncertain
The specialist reconciles the actual instrument to settle the effect on the client's contract.

Reference: CM02; CM03; CM07; CM10

CM02 CM03 CM07 CM10

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

CM-R03 Information types and authority

Ask
Program/data owner

Gather
Customer provided CUI categories/markings, handling instructions, FCI description, contract data lists and export/security restrictions; masked examples where permitted.

Where to ask
Program office, contract data repository

Why it may be needed
Supports the data classification and boundary discussion.

If missing or uncertain
Record who can confirm the designation.

Reference: CM01; CM04; CM06

CM01 CM04 CM06

CM-R04 Boundary and data flow

Ask
IT architect and process owners

Gather
Systems that create, receive, process, store, transmit or protect relevant information; tenant/site/network diagrams, users, interfaces and external transfers.

Where to ask
Architecture, process walkthrough and providers

Why it may be needed
Lets the specialist define candidate in scope assets and dependencies.

If missing or uncertain
List candidate paths, personal accounts and legacy systems for follow up.

Reference: CM08; CM01

CM08 CM01

CM-R05 System security plan and asset facts

Ask
Security lead

Gather
Existing SSP and revision history; asset inventory; proposed asset categories; facilities, endpoints, identity, remote access, backups and security services.

Where to ask
Security repository and asset manager

Why it may be needed
Helps the specialist evaluate actual scope and existing descriptions.

If missing or uncertain
Supply drafts as drafts.

Reference: NI01; CM08

NI01 CM08

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

CM-R06 Providers and cloud responsibilities

Ask
Provider manager

Gather
MSP/MSSP/CSP contracts, service boundaries, customer responsibility matrices, subcontractor access and existing authorization/equivalency evidence requested by the specialist.

Where to ask
Procurement, cloud providers and contract files

Why it may be needed
Clarifies inherited versus client performed work and evidence access.

If missing or uncertain
Ask for exact service/scope and responsibility records.

Reference: CM05; CM08

CM05 CM08

CM-R07 Access and identity records

Ask
IT administrator

Gather
Authorized user/device lists, role approvals, remote/privileged/MFA settings, employee lifecycle records and prior reviews.

Where to ask
Identity, HR, endpoint and application records

Why it may be needed
Enables evidence planning for access and identification/authentication topics.

If missing or uncertain
Provide scoped records through the approved route.

Reference: NI01 access control and identification/authentication

NI01

CM-R08 Configuration and change records

Ask
Infrastructure and development owners

Gather
Baselines, inventory, authorized software, change approvals, configuration reviews and existing patch/vulnerability/remediation records.

Where to ask
Configuration, software and ticket systems

Why it may be needed
Supports configuration, integrity and risk topics.

If missing or uncertain
Log end of support assets and historical settings to trace as follow up items.

Reference: NI01 configuration management, risk assessment and system integrity

NI01

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

CM-R09 Logging and incident records

Ask
Security operations

Gather
Logging policy and actual coverage/retention, alert reviews, time synchronization, incident plans, existing exercises and reporting records when releasable.

Where to ask
SIEM, providers and incident repository

Why it may be needed
Prepares audit/accountability and incident response discussions.

If missing or uncertain
Document logs or periods held elsewhere, with the owner who can reach them.

Reference: NI01 audit and accountability, incident response; CM05

NI01 CM05

CM-R10 Physical and personnel records

Ask
Facilities and HR

Gather
Authorized areas, visitor/access records, personnel screening/separation processes, relevant training and responsibility records.

Where to ask
Facilities, HR and providers

Why it may be needed
Covers nontechnical evidence held by facilities, HR and providers.

If missing or uncertain
Use restricted handling for personnel data and route policy requests to their owner.

Reference: NI01 awareness, personnel security and physical protection

NI01

CM-R11 Media maintenance and transfer records

Ask
IT and operations

Gather
Removable media rules, transfer paths, storage/disposal records, maintenance approvals and remote support restrictions.

Where to ask
IT, operations, service partners

Why it may be needed
Supports discussions of portable copies and service provider work.

If missing or uncertain
Identify any untracked path; the specialist chooses the follow up and evaluates the control.

Reference: NI01 media protection and maintenance

NI01

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

CM-R12 Network and data protection records

Ask
Network and application owners

Gather
Existing diagrams, boundary rules, segmented environments, communications protection, encryption/module descriptions and applicable exception decisions.

Where to ask
Network, application and cryptographic owners

Why it may be needed
Lets the specialist request evidence appropriate to the actual environment.

Reference: NI01 system and communications protection

NI01

CM-R13 Prior assessments and status records

Ask
Security lead and affirming official

Gather
Existing assessment reports, scope/CMMC UID if issued, dates, SPRS records, affirmations, scoring basis and previous government findings.

Where to ask
Authorized SPRS user and assessment repository

Why it may be needed
Distinguishes actual status from a readiness worksheet or marketing claim.

If missing or uncertain
State Not provided or No prior assessment reported, as appropriate.

Reference: CM01; CM04

CM01 CM04

CM-R14 Outstanding actions and artifacts

Ask
Project lead and security owner

Gather
Existing POA&M, owners, dates, supporting evidence, documented constraints and prior closeout records.

Where to ask
Risk/project and assessment repository

Why it may be needed
Helps plan remediation discussion; eligibility and permitted deferrals are specialist decisions.

Reference: CM01 170.21; NI01

CM01 NI01

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

CM-R15 Evidence handling and collection access

Ask
Data owner and receiving specialist

Gather
Approved repository, authorized recipients, artifact retention instructions, provider cooperation, export limits, handling labels and secure review arrangements.

Where to ask
Security, legal and contract administration

Why it may be needed
Keeps sensitive evidence in the controlled repository while the preparation files index it.

If missing or uncertain
Agree the route first, then provide CUI or detailed artifacts through it. Where assessment hashes or retention records apply, follow the applicable instructions.

Reference: CM01 170.17, 170.18; CM05

CM01 CM05

CM-R16 Specialized systems and field access

Ask
Operations and specialist

Gather
OT, test equipment, restricted systems and shared services; owners, support/vendor rules, safe review options and exclusions.

Where to ask
Operations, engineering and providers

Why it may be needed
Makes technical constraints visible before a proposed assessment.

If missing or uncertain
Set a separate scope and permissions with the system owner.

Reference: CM08; NI05

CM08 NI05

Questions for client IT and owners

A useful answer names the actual system, period, supporting record and its coverage. Where the answer sits with someone else, name the person or provider who can give it.

1. Which signed clauses and modifications tell us the required assessment type today?

Suggested responder
Client IT or system owner

Useful supporting record
Contract extracts, effective dates and open conflict log.

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

2. Where does the customer say the CUI comes from, and which category or handling instruction supports that?

Suggested responder
Client IT or system owner

Useful supporting record
Written customer direction and a permitted masked example.

3. Can a relevant file leave the proposed enclave through email, sync, printing, support, backup or personal storage?

Suggested responder
Client IT or system owner

Useful supporting record
A diagram and one actual workflow explanation drawn from how the work is done.

4. Which security services protect the environment and who operates them?

Suggested responder
Client IT or system owner

Useful supporting record
Provider scope and customer responsibility matrix.

5. What controls are planned rather than operating?

Suggested responder
Client IT or system owner

Useful supporting record
Existing SSP/POA&M version and implementation dates.

6. What records are available for the period, and which are only current snapshots?

Suggested responder
Client IT or system owner

Useful supporting record
An evidence period inventory with gaps.

7. Has an assessment or affirmation actually been entered into SPRS?

Suggested responder
Client IT or system owner

Useful supporting record
Authorized export or receipt with the relevant identifier and scope.

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

8. What must the receiving specialist verify before scheduling work?

Suggested responder
Client IT or system owner

Useful supporting record
Boundary, criteria/version, provider cooperation, access and secure evidence decisions.

Facts to confirm and specialist decisions

These are explicit handoff questions, and each one closes with the specialist's written answer, drawing on the records marked Received. Add client specific questions and a responsible person.

CM-Q01 What is the effect of the current suspension/deviation on this actual contract?

Ask
Contracts counsel and authorized contracting contact

Gather
Signed contract and modifications; current deviation including later changes

Resolution needed
Written contract specific interpretation before committing to an assessment path or date.

CM-Q02 Which requirement and assessment revisions and asset boundary should the specialist use?

Ask
Receiving CMMC/NIST specialist

Gather
Contract data types, SSP, diagrams, provider services and official criteria

Resolution needed
Agreed criterion/version and scope, with scoring and certification handled in the formal assessment.

Preparing the handoff

The handoff is ready when the actual contract package and its current amendments are indexed; when the FCI and CUI questions and the boundary and provider gaps remain visible until the specialist closes them; when the security records are grouped by subject and period with planned items labelled as planned; and when the recipient has confirmed the assessment pathway, the correct revision and the handling rules before any formal work begins.

Sources for this package

Official laws/rules establish duties within their scope. Guidance explains programs; NIST supplies methods; vendor documentation describes possible product behavior. The package works alongside the actual contracts, facts, configuration and case orders.

- CM01 CMMC program rule
- CM02 Current CMMC program information

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

- CM03 CMMC Phase II suspension announcement
- CM04 DFARS CMMC clause
- CM05 DFARS safeguarding and cyber incident reporting
- CM06 FAR basic safeguarding
- CM07 Current defense acquisition class deviations
- CM08 CMMC Level 2 scoping guidance
- CM09 CMMC resources and documentation
- CM10 Defense class deviation 2026 O0025 Revision 3
- NI01 NIST SP 800-171 Revision 2
- NI02 NIST SP 800-171 Revision 3
- NI03 NIST SP 800-171A Revision 3
- NI05 NIST SP 800-115

These materials help you prepare and gather information for the professional you bring them to. That professional sets the scope, the records and the conclusions with you.

Source review date: October 18 2026.

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.