What Is CUI, and Where Does It Go in Your Shop?

> *A free DIBGuard scoping worksheet for small defense manufacturers. Print it, fill it in, mark it up, walk it around the floor.*

Read this first

This worksheet helps your shop see where customer technical data — drawings, models, specs, RFQ packages, inspection requirements, programs, travelers — actually goes once it arrives. The goal is to make your CMMC scope visible before you spend heavily on consultants, full-time compliance staff, or assessment preparation.

A few important notes before you start:

- This worksheet is **education and structured note-taking**. It is not legal advice, compliance advice, assessor advice, RPO advice, MSP advice, or consulting. It does not determine whether anything in your shop is acceptable under CMMC or NIST SP 800-171.
- Your organization remains responsible for its own CMMC scope decisions, control implementations, evidence, SPRS score, affirmations, and assessment outcomes.
- Findings from this worksheet should be reviewed with qualified advisors — your MSP or internal IT team, a Registered Practitioner (RP/RPO), an attorney, or a C3PAO — before they inform formal decisions.
- This worksheet does not collect or store any of your data. Anything you write on it stays with you.

A note on terminology: throughout this worksheet, "CUI" means Controlled Unclassified Information as defined by the National Archives CUI program and referenced in DFARS 252.204-7012. CMMC certification levels and assessment requirements are defined under DFARS Subpart 204.75 and 32 CFR Part 170. For authoritative source links, see DoD CIO's CMMC pages.

---

1. What Is CUI?

CUI is sensitive government-related information that is not classified but still has handling rules. If a defense customer sends you drawings, models, specs, inspection requirements, RFQ packages, flow-down clauses, or controlled technical data, you should not assume those are ordinary job files.

Working with defense or aerospace customers does **not** automatically mean every file you receive is CUI. It does mean you need a deliberate way to identify what is, mark it, and handle it correctly.

Examples of customer materials that **may** need controlled handling (your customer, your contract, and your advisors determine the actual classification):

- Customer drawings (2D prints, dimensioned drawings)
- 3D models and model-based definition files
- CAD/CAM files
- RFQ packages (the bid package itself, not just public solicitation pages)
- Technical data packages
- Specifications and standards referenced as controlled
- Inspection requirements and inspection plans
- Quality clauses and quality flow-downs
- Special-process requirements (heat treat profiles, coating specs, etc.)
- CNC programs derived from controlled drawings
- Ballooned drawings used for inspection
- Setup sheets that reproduce dimensional content
- Work instructions that include controlled technical detail
- Vendor RFQs that include any of the above
- Customer portal downloads (the file is what matters, not the portal)
- Screenshots, photos, or scans of any of the above

If you are unsure, ask the customer in writing. Their answer becomes part of your record.

---

2. How Does Customer Technical Data First Arrive?

Check every channel that has happened in the last 90 days, even once.

- ☐ Email attachment

- [ ] Customer portal download
- [ ] Secure file share (SFTP, link service, or similar)
- [ ] Cloud folder or share link (Google Drive, OneDrive, Dropbox, Box, etc.)
- [ ] Physical media (USB drive, external hard drive, DVD)
- [ ] Paper packet (mailed, hand-delivered, dropped off)
- [ ] Vendor or customer handoff in person
- [ ] Other: _____

---

3. Where Is It Supposed To Go First?

After it arrives, where does the file actually land first? Be honest. If different files go different places, check all that apply.

- [ ] Approved CUI folder or repository
- [ ] Email inbox (and stays there)
- [ ] Local Desktop or Downloads folder
- [ ] Shared drive (general, not CUI-specific)
- [ ] ERP / MRP / QMS attachment
- [ ] CAD/CAM or programming workstation (local files)
- [ ] Printed packet (goes straight to paper)
- [ ] Customer portal only (you read it there, never download)
- [ ] Unsure
- [ ] Other: _____

> *If the answer is not one approved location, your CUI path may already be branching.*

---

4. Who Needs To See It?

Write the **role or function**, not just the job title. In a small shop one person may wear several hats; record what they do, not what their badge says.

Function	Who in your shop performs this	Do they need the full file, or only extracted info?
Owner / management		
Sales		
Estimating		
Engineering / manufacturing engineering		
Purchasing / materials		
Programming / CAD/CAM		
Machinist		
Quality / inspection		
Production planning		
Outside-processing coordinator		
Shipping / export-related role		
MSP or internal IT		
Other: _____		

> *In small shops, one person may wear several hats. Record the function, not just the job title. The same person may appear on several rows.*

---

5. Print Reality Check

If your team prints drawings, models, specs, travelers, or inspection packets, that may be necessary. Inspection in particular often runs on paper. We're not here to tell you to stop printing.

It also means **paper becomes part of your CUI process** and can make your CMMC scope more complex. A printed CUI page is still CUI, and the way it moves through your shop becomes part of what you'll need to document.

Walk through these questions honestly. "I'm not sure" is a valid answer — write it down.

- Who is allowed to print CUI? _____

- Where does CUI print (which printer, which area)? _____
- Can a printed CUI page sit unattended on the printer? _____
- How is printed CUI marked (banner, header, footer, stamp, none)? _____
- Where is printed CUI stored during the job? _____
- Can printed CUI leave the facility (off-site machinist, home review, vendor visit)? ____
- Is printed CUI locked up overnight or when not in active use? _____
- How is printed CUI destroyed (cross-cut shred, burn bag, contracted service)? _____
- Is destruction logged (date, who, what)? _____
- Who owns the printed packet or traveler while it is active on the floor? _____

---

6. What New Copies Or Notes Get Created?

You may protect the source drawing carefully and still create uncontrolled derivative artifacts that carry the same sensitive technical detail. Marked-up drawings, cost sheets, vendor RFQs, and inspection notes can all reproduce the controlled content of the original.

Principle: minimum necessary extraction is safer than copying the full technical package into new places. A vendor RFQ that says "0.500 +/- 0.001 OD on 17-4 PH bar, qty 50" is generally lower risk than the same RFQ with the customer's full drawing attached. Your contract and your advisors determine what counts as acceptable extraction.

Check what your shop creates today (pre-award and post-award).

- [ ] Marked-up drawings
- [ ] Screenshots of drawings, models, or screens
- [ ] Printed packets and travelers (covered in section 5 too)
- [ ] Inspection notes that quote dimensions or tolerances
- [ ] Cost sheets with embedded customer technical detail
- [ ] Material takeoffs that reproduce the geometry
- [ ] Vendor RFQs that include the source drawing
- [ ] Setup sheets that reproduce dimensional content
- [ ] Work instructions that include controlled technical detail
- [ ] Photos of drawings, parts on the machine, or inspection screens
- [ ] Whiteboard or conference-room notes with controlled detail
- [ ] Other: _____

---

7. Does It Leave The Building Or Go To Outside Vendors?

Most small machine shops use outside processes for steps they don't perform internally. Each one is a place where CUI may leave your boundary.

Common outside processes (check those you use):

- ☐ Coating
- ☐ Plating
- ☐ Forming or bending
- ☐ Heat treating
- ☐ Painting or finishing
- ☐ Assembly
- ☐ Testing
- ☐ Certification (NADCAP, AS9100, customer-specific)
- ☐ Calibration
- ☐ Other specialized operations: _____

For each outside process you checked, work through the questions below. (One worksheet column per vendor / process is fine; copy the table if you need more rows.)

Question	Vendor / Process A	Vendor / Process B
What information is sent? (full drawing/model/spec, or only extracted process detail?)		
Is it the full technical package or only minimum necessary?		
How is it sent (email, portal, SFTP, paper, in person)?		
Who approves the share before it goes out?		
Is the vendor approved or verified for the type of information sent?		
Are flow-down requirements included where needed (DFARS 252.204-7012, CMMC level requirements, etc.)?		
Is the share logged (date, file, recipient, approver)?		
Where is proof of the share stored?		

8. Risky Paths To Notice

This is **not a compliance score.** It is a quick way to see how many pathways your shop may need to document.

Where does your shop sit, roughly?

Simpler:

- One approved digital location for CUI
- Limited, defined access
- No printing of CUI
- No removable media
- No uncontrolled local copies on laptops or workstations
- Few or no external shares

More complex:

- Multiple roles or departments use the data
- But only through defined systems, defined access paths, and written rules

Most complex:

- Printing is allowed, common, or unmanaged
- Local copies and downloads on laptops or workstations
- Off-site laptop access, including home or travel
- CUI sits in email storage or unmanaged inboxes
- Outside vendor sharing is informal or undocumented
- ERP / MRP / QMS attachments include controlled content
- Shop-floor systems (CNC controllers, OT, test equipment) hold controlled content
- Printers, scanners, or copiers store digital images of CUI
- Inspection areas hold drawings, marked prints, or models
- Mobile phone photos of drawings, parts, or screens
- Whiteboards or conference-room notes with controlled content

> *The goal is not always to make every path disappear. The goal is to know which paths exist, decide which ones are necessary, and document how each one is controlled.*

9. Questions To Ask Your MSP, Internal IT, Or Advisor

Bring this worksheet to whoever supports your IT and security — an outside MSP, an internal IT team, an RP/RPO, or a CMMC consultant. They may already have answers to most of these questions, and where they don't, your conversation just got more useful.

- Where does CUI or suspected CUI live today across our systems?
- Who can access it? (people, roles, groups)
- How is access approved and reviewed, and how often?
- Is multi-factor authentication enforced for systems that touch CUI?
- Are logs enabled, retained, and reviewed for those systems?
- Do backups include CUI, and where do those backups live?
- Is sync or offline access controlled (laptops, tablets, phones)?
- Are local downloads, USB or removable media, and printing technically restricted, or only restricted by policy?
- What inherited controls do we rely on from cloud, security, or managed-service providers?
- What evidence can you provide for those controls, without exposing sensitive data unnecessarily?
- Are any cloud services we use for CUI FedRAMP-authorized (or otherwise documented as appropriate for CUI) under DFARS 252.204-7012?
- Do you support other customers handling CUI / CMMC requirements?
- Are you comfortable with CMMC terms like CUI Asset, Security Protection Asset, Contractor Risk Managed Asset (CRMA), Specialized Asset, SSP, SPRS, POA&M, and shared responsibility matrix?
- How quickly can you respond to evidence requests or configuration questions during an assessment readiness window?

These questions do not assume your MSP or IT team is the problem. They help you and your advisors see the same picture.

---

10. Proof Reminder

For any path you keep — every system, every printed packet, every outside share — you will eventually need proof that the process exists and is followed. Documentation, training records, access lists, logs, review notes, destruction records.

You don't have to produce all of that today. But it's worth knowing now which paths will need evidence later.

---

11. Next Step

Turn this worksheet into a CUI flow diagram and starter SSP package with DIBGuard Foundation.

DIBGuard Foundation is a guided CMMC scoping workbook for manufacturers. It helps you:

- Map CUI flow through your shop
- Identify the choices that expand scope
- Build a starter asset inventory (CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and optionally Out of Scope)
- Prepare draft documentation for review with your MSP, consultant, RPO, attorney, assessor, or internal team

Foundation is software. It produces a structured scope map, asset inventory, CUI-flow narrative, evidence references, and starter SSP language grounded in your shop's actual workflow.

Pricing: Foundation is **$3,600/year**, with a 90-day full-refund window. There is no free product tier, and there are no free pilots.

> *DIBGuard is software, not legal, compliance, consulting, MSP, RPO, or assessment services. Your organization remains responsible for its CMMC interpretations, implementation, evidence, SPRS score, and assessment outcomes.*

Visit dibguard.com when you're ready to map this into a working scope package.
