CUI Data Spillage

How Defense Subcontractors Discover It, Contain It, and Resolve It in the CMMC Era

David W. Koran

CyberAB Registered Practitioner Advanced

September 5, 2026

Summary

In plain terms: a purchasing clerk trying to keep parts moving can email a controlled technical package to two suppliers and put the company into a federal reporting obligation before lunch, with no hacker involved. Deleting the email afterward can destroy the best evidence of what happened while leaving other copies untouched. This paper follows one fictional spill from a Thursday afternoon send to a defensible closure, and shows the difference between a response that survives scrutiny and one that creates a second problem.

This paper examines Controlled Unclassified Information (CUI) spillage at small and midsize defense manufacturers. It grounds the discussion in the public record, including the 2023 export-control settlement with 3D Systems Corp. that began in a routine quoting workflow, and then uses a fictional composite company, Cogswell Cogs, to walk through how a spill begins in ordinary purchasing work, how it is discovered, why an inadvertent electronic disclosure can be a reportable cyber incident under DFARS 252.204-7012 without any malicious activity, and what resolution requires: scoping, evidence preservation, timely reporting, supplier coordination, verified remediation, and an honest closure record. The same starting facts are handled two ways. The wrong response deletes evidence, accepts verbal assurances, and runs out the reporting clock. The right response preserves first, reports on the facts available, and documents what the company knows and what it can't establish.

The Spill That Starts with a Purchase Order

A CUI spill doesn't need an attacker. It can begin with a request for quote, a purchase order, a manufacturing traveler, or a drawing sent to a plater. The information leaves the protected environment because someone doing their job put it somewhere convenient, and every system it touches from that point forward becomes part of the problem. The company has lost control of its information through an ordinary business activity, and nothing looks broken.

Resolving a spill means answering five questions: what information was exposed, where it traveled, who could access it, what obligations apply, and what evidence supports containment and corrective action. Deleting the original attachment answers none of them. It removes one copy from one location and, if done carelessly, destroys the record that would have answered the other four.

CUI isn't the same thing as ordinary proprietary information, though the two can overlap. Proprietary information may be protected through contracts,

trade secret law, and the company's own safeguards. CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. The governing framework is 32 CFR Part 2002 and the categories are defined in the NARA CUI Registry, which includes a category for proprietary business information; a company's own proprietary designation alone doesn't establish CUI status, and CUI status doesn't depend on that designation. The safeguarding obligation reaches the contractor through the contract, and it doesn't evaporate because the disclosure was accidental or because the recipient was a trusted supplier.

A CUI handling incident is also not automatically a reportable cyber incident, and a reportable cyber incident doesn't require malice. DFARS 252.204-7012 defines a cyber incident as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system or the information residing in it, and it defines compromise to include disclosure of information to unauthorized persons. An email that carries covered defense information to people who have no authorization to hold it can meet that definition on its face. A paper traveler left on a break room table can't, because no computer network was involved, though it may still trigger other obligations. Each incident has to be assessed against the definitions in the actual contract, not against an intuition that reporting is for hackers.

The Public Record

None of this is hypothetical, and the closest documented case to the scenario in this paper came out of a quoting workflow. In February 2023, the Commerce Department's Bureau of Industry and Security imposed a $2,777,750 administrative penalty on 3D Systems Corp., which had regularly emailed customer design documents, blueprints, and technical specifications to its then-subsidiary's office in Guangzhou, China, to generate price quotes. The emails included controlled drawings for military electronics and for spacecraft development and repair, sent without the required licenses and without the knowledge of the U.S. customers who had requested the quotes. Copies also reached a mirrored server in Germany that stored employee email. At bottom, this case and the fictional spill in this paper were discovered the same way: a customer noticed a problem in routine supplier correspondence. Here, a defense contractor came forward after noticing that a price quotation indicated the quoted parts would be manufactured in Asia using controlled technology. The settlement required a third-party compliance consultant and two audits alongside the penalty, with parallel resolutions at the State Department and the Justice Department. That was an export-control enforcement action under the Export Administration Regulations, not a DFARS ruling, and it should be described that way. The

mechanics, though, are the ones this paper is about: a routine quoting process moved controlled technical data into another company's replicated systems, invisible to the customer, until a person reading a quote noticed.

The government's own audit record documents the pattern. The DoD Inspector General reported in DODIG-2019-105 that between March 2015 and June 2018, 126 contractors reported 248 security incidents to the DoD Cyber Crime Center, and the reported incident types included inadvertent disclosure of information alongside network intrusions, stolen equipment, and data exfiltration. Inadvertent disclosure sits in the Department's incident ledger next to hacking. The same audit documented a spillage of classified information into a contractor's unclassified commercial cloud, internal network, and webmail environments, where neither the agency nor the contractor acted promptly and the information remained unprotected for almost two years. That case involved classified information, whose handling requirements differ from CUI and don't transfer wholesale, but the lesson about incomplete containment and follow-through transfers exactly.

Enforcement has also reached companies where the public announcements establish no actual theft or disclosure. In March 2025, MORSECORP Inc. agreed to pay $4.6 million to resolve False Claims Act allegations, admitting among other facts that it used a third-party email host without requiring protections equivalent to the FedRAMP Moderate baseline or the DoD's requirements for incident reporting and media preservation, that it hadn't fully implemented NIST SP 800-171, and that it reported a summary score of 104 when a consultant later measured it at negative 142 (-142). The Justice Department's announcement establishes no actual data theft or specific unauthorized disclosure; the unsuitable systems and the inaccurate representations were the case. On September 1, 2026, Honeywell Aerospace Inc. agreed to pay $2,042,518 to resolve allegations of NIST SP 800-171 noncompliance on one network between April 2020 and December 2023, allegations only, with no determination of liability. Both cases arose from whistleblower suits, which is worth absorbing: the government learns about unsuitable systems through people and subpoenas, not just through breaches, and the suitability of every system the spilled package lands on in this paper's example is not a technicality.

The cases also show that the company isn't the only party positioned to discover its spill, and often isn't the first. The government can learn of one through a whistleblower or a qui tam suit, as it did with MORSECORP and Honeywell; through a customer who notices something in routine correspondence, as it did with 3D Systems; through another company's incident report, since a supplier or prime that reports its own incident identifies the affected contracts and DC3 routes the report to the contracting officers named on it; through its own audits and assessments, which is how the two-year classified spill entered the public record; through a damage assessment of another company's incident that turns up data in unexpected

places; or through threat intelligence when spilled material surfaces where the government or its partners are looking. Investigations also run backward: a drawing recovered from a compromised system, a seized device, or an export prosecution carries its title block, drawing numbers, markings, and distribution statements, and those identifiers can let investigators trace it to the contract and the company it came from, whether or not that company ever knew it was gone. The same distinctive identifiers this paper later recommends for finding copies work just as well in the other direction. MORSECORP didn't correct its score until after a subpoena arrived. The practical consequence for a company like Cogswell Cogs is that discovery timing isn't fully in its control, and the version of events that reaches the government first shouldn't be someone else's.

The Department's own training treats CUI incidents as a named, documented category. The CDSE unauthorized disclosure student guide defines a data spill as a willful, negligent, or inadvertent disclosure of classified information or CUI transferred onto an information system not accredited at the appropriate level, and presents the 2015 OPM breach as a significant CUI incident: personnel files of 4.2 million current and former federal employees and background investigation records of 21.5 million individuals. The facts differ from a machine shop's, personnel data taken by intrusion rather than drawings emailed to a plater, but the category is the same. No named plater or heat treater case documented end to end from discovery through verified closure surfaced in the sources reviewed for this paper. That's why the rest of this paper demonstrates the response process through a constructed example: the discovery and enforcement mechanics above are real, and the process that follows is what they demand.

Cogswell Cogs

Cogswell Cogs is a fictional composite company. It doesn't describe any actual firm, and the incident that follows is constructed for instruction. It is built to look like hundreds of real shops.

The company employs about 85 people at one manufacturing facility and makes precision components for defense aerospace customers on roughly 20 CNC machines, several of them old enough that their controllers predate the compliance conversation entirely. Plating, heat treatment, and some inspection go to outside suppliers. A small internal IT function is backed by an outside managed service provider, and the operations manager coordinates cybersecurity compliance. Engineering keeps controlled drawings and technical packages in a restricted environment. Purchasing runs on a separate business email system and an ERP platform, and when production deadlines press, employees move documents between the two environments, because the restricted environment is where the drawings live and the ERP is where the purchase orders live.

Supplier approval at Cogswell Cogs has historically turned on quality, price, delivery, and special-process qualifications, while verification of how suppliers handle information has been inconsistent. A supplier can hold a special-process accreditation and deliver conforming parts for a decade while storing customer drawings on a shared office computer that anyone in the front office can open. Quality approval establishes that the supplier can make the part. It establishes nothing about where the drawing goes after it arrives.

For this case, the relevant prime contracts and subcontracts include DFARS 252.204-7012, and the technical package at the center of the incident has been confirmed as covered defense information through the contract and the customer, not inferred from a filename or a marking block. Markings are evidence of status, not the source of it, and a package doesn't become uncontrolled because someone saved it under a new name.

The Incident and Its Discovery

On a Thursday afternoon, a purchasing employee downloads a controlled technical package from engineering's protected environment, attaches the entire package to an ERP purchase order, and emails it to the plater and the heat treater. The reasoning is entirely practical: send everything, prevent questions, avoid a delivery delay. Both suppliers legitimately need some controlled technical information to do their work. Neither needs the full package, which includes drawings and manufacturing details unrelated to plating or heat treatment.

The investigation will eventually establish six facts. The package remained in the purchasing employee's downloads folder. A copy was stored as an attachment in the business ERP system. The email and its attachments entered ordinary mail retention and backup systems whose suitability for this information had never been established. The plater saved the package to a shared office computer accessible to personnel with no established need for it. A plater employee forwarded the package to an outside estimating consultant without approval. The heat treater downloaded it to an office laptop that synchronized with a cloud account outside any approved workflow.

None of this is known on Thursday, or on Friday, because nothing has gone wrong in any visible way. The spill sits quietly in six locations across three companies and one consultant's inbox.

At 9:15 a.m. on Monday, Cogswell Cogs' quality manager receives an ordinary email from the plater that happens to contain one of the controlled drawings, recognizes that the package bypassed the approved transfer process, and raises the concern. That is the discovery, and at that moment the company knows three things: one controlled drawing is sitting in an

unprotected mailbox, at least one supplier received material through the wrong channel, and somebody sent it. Everything else, the downloads folder, the ERP copy, the backups, the shared computer, the consultant, the synchronized laptop, is still invisible and will surface only through investigation over the following days. A response plan that assumes the company knows the full distribution at discovery describes an incident that doesn't happen in real life.

Why this one is reportable

For this case, assume the company's documented assessment establishes a reportable cyber incident, and look at the facts that support the conclusion. Three findings are distinct even where they overlap, and establishing one doesn't automatically establish the others: a system whose safeguards were never evaluated, a system that fails the applicable safeguards, and a cyber incident. Here the documented assessment supports each on its own evidence. Covered defense information was transmitted over an email system never evaluated for it, came to rest on systems outside the safeguarding the contract requires, and was disclosed to people with no lawful government purpose or authorization to access it: front office personnel at the plater and an estimating consultant with no relationship to the contract at all. Under the clause definitions, disclosure of covered defense information to unauthorized persons through computer networks is a compromise, and every action here ran through computer networks. No malware, intrusion, or adversary is required, and the definition doesn't require proof that any recipient opened a file. The assessment is each company's to make and document against its own contracts and facts; the point of the example is that these facts, honestly assessed, clear the threshold.

The Wrong Response

Here is what happens when management treats the spill as an embarrassing paperwork problem.

Monday morning, purchasing calls both suppliers and asks them to delete the email, and both agree. The operations manager accepts the verbal assurances and writes a note that the files are gone. IT deletes the attachment from the ERP and clears the purchasing employee's downloads folder, tidying up before anyone thinks about preserving evidence. Nobody asks about forwarding, cloud synchronization, shared computers, or backups, because nobody has imagined them. Management concludes there is no incident: the recipients are established suppliers, there is no hacker, and nothing was stolen. Notification is postponed until Friday while management tries to find out whether anyone actually opened the documents. On Friday the event is closed with a reminder email to employees about using the file portal.

Each of those decisions costs something specific. The deletion request reaches two mailboxes and misses the shared office computer, the consultant's copy, and the synchronized cloud account, because the people deleting don't know those copies exist either. The verbal assurances are sincere and incomplete: the plater's contact genuinely believes the email is gone and genuinely doesn't know a coworker forwarded it. Deleting the ERP attachment and the downloads folder destroys the cleanest record of exactly what was sent, in which versions, and when, which is the evidence needed to scope every other copy. The conclusion that established suppliers plus no hacker equals no incident substitutes a feeling for the clause definition, which turns on disclosure to unauthorized persons, not on the attacker's existence. The wait until Friday chases a question the clause doesn't ask, whether anyone opened the files, while consuming the 72-hour window it does impose. And the closing reminder email documents that the company saw the event, decided it was minor, and moved on.

None of this means the spill automatically ends in contract termination, loss of certification, or a False Claims Act case. Consequences depend on the facts, the obligations in the specific contracts, the representations the company has made about its systems, and the quality of its response. What the wrong response reliably produces is a company that can't answer basic questions with evidence: asked what was disclosed, it estimates; asked where the copies went, it repeats assurances; asked what it did in the first 72 hours, it describes deletions it can't reconstruct. Whatever the ultimate exposure, that position weakens every conversation that follows with the customer, the government, and counsel.

The Right Response

Now run the same Monday morning again, with the same facts and a company that treats the event as an incident from the first hour.

The first hour

The operations manager takes ownership as response lead and opens an incident record: discovery time of 9:15 a.m. Monday, the facts known so far, the contracts potentially affected, and every action taken from this point forward with a timestamp. IT and the managed service provider are brought in immediately; operations, contracts, supplier management, and legal counsel are engaged as the facts warrant. Further distribution through the affected workflow stops: no more technical packages leave through purchasing email while the incident is open. Access is restricted and sharing revoked where feasible. Employees and both suppliers receive a written direction to preserve relevant messages and files and to make no deletions except in coordination with the response. A secure channel is established for

incident coordination, because discussing the spill by attaching the spilled documents to more ordinary email would extend it.

Containment and preservation proceed together, and neither waits for the other to finish. The company doesn't leave an active sharing link open while it waits for a forensic image, and it doesn't wipe a laptop to feel contained. It cuts off ongoing exposure now, preserves what exists now, and keeps both actions in the record.

The first business day

By the end of Monday the responders confirm what information is involved and which contracts apply, working from engineering's records of the package contents and the purchase orders that carry the DFARS clause. They identify the affected files and versions, the accounts and systems the package touched, the two suppliers, and the possibility of further recipients not yet found. Qualified personnel preserve the relevant messages with full headers, audit records, transfer logs, and system evidence before anything is altered. They review the ERP attachment store, the downloads folder, shared folders, synchronization services, and available mail retention records, and ask each supplier what evidence it can actually produce about receipt, storage, and onward movement. They evaluate reporting promptly while the investigation continues, rather than treating a complete investigation as a precondition for a report. And they record uncertainty as uncertainty: where a log doesn't exist, the record says visibility is absent, not that access didn't occur.

The following days and weeks

The investigation widens as it should. Supplier cooperation surfaces the consultant forward and the synchronized cloud account, and each new repository goes into scope. Remediation at the suppliers is coordinated and authorized, performed by the suppliers or their service providers with Cogswell Cogs verifying. Unauthorized working copies are removed once preservation requirements and any holds permit, and each removal is verified with evidence rather than assumed from a promise. An approved transfer workflow is restored so production continues through the incident. Open items, retained evidence, and restricted backups go onto a tracked list with owners, and the record accumulates toward a closure decision management can actually defend.

Operationally, containment stays proportionate: this spill lived in email, an ERP, office endpoints, and supplier systems, so the CNC machines keep cutting. Had controlled drawings or part programs moved onto a DNC server or a machine controller, the response would isolate that path specifically, verify before touching production controllers, and preserve before deleting there just as anywhere else. For a spill like this one, blanket disconnection of the shop floor isn't containment; it is a second incident with a delivery

schedule attached. Broader isolation can be warranted where the facts show the production network itself is affected.

Reporting: The Clock, the Portal, and the Record

Where DFARS 252.204-7012 applies and its threshold is met, the contractor rapidly reports the cyber incident to the Department of Defense within 72 hours of discovery. Those are elapsed hours, not business hours. Discovery at 9:15 a.m. Monday produces a deadline of 9:15 a.m. Thursday in the same time zone. The clock started when the quality manager recognized the problem, not when management finished deciding what to make of it. Internal escalation doesn't restart it, and a call to the customer doesn't substitute for the required government report.

Subcontractors report directly: an affected subcontractor submits its own report to the Department and provides the automatically assigned incident report number to the next higher contractual tier as soon as practicable. The plater and the heat treater each assess their own obligations under their own subcontracts and their own discovery timing; no company's report discharges another's.

Reporting runs through the DoD Cyber Crime Center. The contractor submits an Incident Collection Format through DC3's DIB cybersecurity reporting site, which requires a DoD-approved medium assurance certificate. That certificate takes days to obtain, so the time to get one is before an incident. A company that discovers an incident without portal credentials should contact DC3 for reporting assistance rather than letting the deadline pass while a certificate application processes. The initial report carries the facts available at submission, and a follow-on report supplements it as the investigation develops.

The report isn't the end of the preservation obligation. The clause requires the contractor to preserve and protect images of all known affected information systems and all relevant monitoring and packet capture data for at least 90 days from submission of the report, so the Department can decide whether it wants access for a damage assessment. Preservation therefore outlasts cleanup, and cleanup has to be planned around it.

Separately, the company identifies any additional notifications: prime contract flowdowns that require notice to the customer, quality clauses, nondisclosure agreements, and any other regime the facts implicate. The direction runs both ways: a paper handling incident with no network involvement doesn't inherit the 72-hour cyber rule, and an electronic

disclosure that meets the definition doesn’t escape it because it feels administrative.

Working with the Plater and the Heat Treater

Supplier coordination is where scoping succeeds or fails, because most of the copies are in other companies’ systems. Cogswell Cogs needs specific answers from each supplier. Who received, opened, downloaded, printed, or forwarded the information? Which accounts, devices, shared folders, services, and backups may contain it? Was it sent to another company, a consultant, or a personal account? What access and activity records exist, and when do they expire? What containment has already been completed? Who at the supplier owns preservation, reporting, and corrective action? And for every answer, what evidence substantiates it? That last question separates this exercise from the verbal assurances in the wrong response, because an answer without evidence is a starting point rather than a finding.

Small suppliers often can’t answer these questions with tools, because they don’t have the tools. A 12-person plating shop may have no internal IT at all. The practical path is proportionate: the supplier’s evidence might be a mailbox search run with a part-time IT consultant, a screenshot of the shared folder before and after removal, and a signed statement of who had access to the office computer. These records supplement rather than replace the preservation the clause requires; limited IT resources don’t remove the obligation to preserve system images and monitoring data where it applies. Cogswell Cogs can offer authorized technical assistance, for example its managed service provider working with the supplier’s written permission. What it can’t do is assume authority to access another company’s systems because its data is on them; cooperation is obtained, documented, and assisted.

If a supplier refuses to cooperate, or can’t establish that it can handle the information suitably, the response escalates through management and contracts: further transfers of controlled information stop, the relationship question goes to purchasing and quality leadership, and an alternative supplier is evaluated for the work. Keep the two decisions separate: incident remediation asks whether this spill got cleaned up and evidenced. Supplier qualification asks whether this supplier should receive controlled information again. A supplier can pass the first and fail the second.

Finding the Copies: Tools and Their Limits

This spill was discovered by a person, not a product. An employee recognized something out of place and said so, which remains one of the most valuable discovery mechanisms a small manufacturer has. Around that sit supplier disclosures, access reviews, email investigations and message traces, endpoint tools where deployed, and targeted data discovery across the systems the company can reach.

Digital fingerprinting deserves specific treatment because it is genuinely useful and routinely oversold. An exact cryptographic hash of each file in the spilled package will find byte-identical copies wherever the company can search, including renamed copies, which is how the ERP attachment and the downloads folder copy are confirmed quickly and how, with the plater's cooperation, the shared computer copy is matched. But any modification, a resave, a format conversion, an extracted page, changes the hash, so modified files need other methods. Content matching can identify reused text and recognizable portions of known documents, and optical character recognition can extend the search to scanned pages and screenshots where the tooling supports it. Distinctive strings carry a lot of weight in a machine shop: drawing numbers, part numbers, project identifiers, and unusual technical text make effective search terms, and a drawing-number search of the plater's mailbox is what surfaces the consultant forward.

The limits are as important as the capabilities. Common title block text produces false positives. Degraded scans, CAD files, and derived manufacturing data such as post-processor output are missed by text methods never designed for them. Coverage extends only to systems the company can lawfully search, which excludes the consultant's inbox absent cooperation. A fingerprinting system also doesn't determine legal CUI status. And the reference repository, its indexes, the search results, and the incident evidence collectively describe the company's most sensitive information and must be protected accordingly. Used with those limits acknowledged, these methods let Cogswell Cogs locate copies it would otherwise never find. They don't support a claim that every copy has been found, and the closure record shouldn't make one.

Cleanup, Backups, and Defensible Closure

Ordinary deletion isn't evidence of removal. A deleted file sits in a recycle bin, a deleted email persists in mail retention stores, version history keeps prior copies, and synchronized devices restore what the desktop removed.

Temporary files, printed copies, backups, and provider-managed storage all hold what the visible file system no longer shows. Recalling an email can't establish removal of every copy, download, forward, or retained version, and deletion alone doesn't establish complete remediation or produce anything that can be shown to anyone later.

The correct sequence runs preservation first, then sanitization chosen to fit the media and the risk. Once the evidence required by the clause and any legal holds is preserved and protected, unauthorized copies are removed using methods appropriate to what they sit on, drawing on the concepts in NIST SP 800-88 Rev. 2 for media sanitization. What the plan doesn't include is indiscriminate wiping or destruction of backups. Backups usually serve other retention requirements and other data, and destroying them to eliminate one spilled package trades a contained problem for an uncontained one.

Where a retained backup can't immediately be altered, the workable interim position is restriction: access to the backup set is limited and logged, its retention and eventual disposition are documented, and restoration procedures are controlled so a routine restore doesn't quietly reintroduce the spilled package. These measures require evaluation against the applicable requirements in each case. They manage the residual copy; they don't transform an unsuitable system into a compliant one, and the closure record should describe them as the former.

Closure itself is a sequence of distinct states, and collapsing them is how companies close too early. Containment means further movement has stopped. Operational recovery means an approved workflow is running. Corrective action completion means the fixes are done and verified. Final closure means management has decided, on a documented basis, that the incident is resolved. Evidence preservation can continue past all of the intermediate states, since the 90-day minimum runs from the report and holds may run longer.

The closure record identifies the information, systems, recipients, and contracts affected; the timeline and the investigation methods used; the findings and the visibility gaps that remain; the notifications made and the report references; the evidence retained and the requirements governing its retention; the remediation performed and how it was verified; the corrective actions completed at each supplier; and the restrictions still in force with a named owner for each. It ends with management's documented closure decision. What it never contains is a claim of complete eradication or an assertion that no disclosure occurred, unless the evidence actually supports the claim. An honest record that says the consultant's copy was confirmed deleted with supporting evidence, while the expired mail logs leave a two-day visibility gap, is worth more than a confident record that later proves wrong.

The Same Problem in Other Clothes

The purchasing email is one shape of a general problem. Five minutes with any of the following shows the same structure: discovery, immediate action, scoping, a reporting assessment against the actual contract, and closure evidence.

Controlled drawings copied to a legacy CNC workstation typically surface during an access review, a network scan, or machine maintenance. The immediate action is to restrict the share or the network path, not to shut down a machine mid-cycle. Scoping asks which files, how they got there, and whether the workstation is reachable from anywhere it shouldn't be. Reporting depends on the facts: an undocumented in-scope system and a reportable incident are different findings, and they can coexist, since the clause's definition of compromise reaches certain security-policy violations without requiring proof that anyone opened a file. Closure needs verified removal or documented controls that make the workstation a suitable home.

A manufacturing traveler left in a common area is usually found by the next person through the room. Retrieve it, establish the exposure window and who had access, and correct the handling practice. With no network involved, this is a handling incident assessed under physical protection and any customer notice obligations, not the 72-hour cyber rule. The closure evidence is the record itself: what, where, how long, who, and what changed.

A smartphone photograph of a drawing sent through a personal messaging account is typically discovered by report or admission. Scoping is hard because personal accounts sit outside any visibility the company has, and the reporting assessment must be made seriously because the disclosure is electronic and outside every approved system. Closure will candidly document limited verification: a deletion the company was shown, on an account it can't audit.

Technical information uploaded to an unauthorized AI service or a free online converter is discovered through browser history, proxy or firewall logs, or an employee explaining how a file changed format. Containment narrows to the service's own deletion mechanisms and terms, which vary and rarely satisfy. The reporting assessment turns on what the information was and where the service put it. Corrective action is blocking, an approved alternative for the legitimate need the employee actually had, and training.

Contractor-generated inspection or manufacturing data with unclear markings, dimensional reports derived from a controlled drawing, for instance, is a classification question before it is an incident. Missing markings don't make information uncontrolled, and not every manufacturing record is CUI. The interim position is to handle the data as controlled while the question is clarified through the contractual channel and, where needed, the

government customer, rather than resolving the ambiguity by assumption in either direction.

A historical spill discovered after the relevant access logs have expired is the hardest case, because the visibility gap is permanent. The clock considerations run from when the company discovered the event, and the scoping record states plainly which questions can no longer be answered. Closure documents the gap as a gap, which is uncomfortable and honest, and the second quality is the one that holds up.

Prevention That Fits a Machine Shop

The purchasing employee in this story wasn't careless; the employee moved information through the path the company's own systems made easiest. Prevention means changing the path rather than admonishing the person.

Start with what suppliers actually need. A plater needs plating callouts, relevant dimensions, and process specifications, not the complete technical package. Reduced packages produced through an authorized technical and CUI review shrink every future spill before it happens, and the review preserves controlled status and required markings on what does go out. Removing a marking doesn't itself decontrol CUI; under 32 CFR Part 2002 decontrol follows the applicable authority and authorized process, not whoever holds the delete key in a PDF editor. Transfers move through approved methods into recipient environments verified as suitable, and supplier readiness is checked before release rather than assumed from a quality rating. The purchasing workflow itself gets rebuilt so the ERP doesn't invite uncontrolled attachment of whatever engineering holds, and so the compliant path is also the convenient one.

Then invest in the response the company hopes never to use. Train employees to report mistakes promptly, and treat the prompt report as the behavior being rewarded: the Monday discovery in this paper worked because a quality manager spoke up within minutes. Exercise the response plan with purchasing, production, IT, and the critical suppliers, because the first hour goes very differently when people have practiced it. Keep procedures, system documentation, and corrective action records current as the workflow changes.

Two cautions complete the picture: a secure transfer portal is a real improvement and an incomplete one, because transfer security alone doesn't establish adequate protection after the recipient downloads the file; the recipient's environment still matters. And CMMC assessment status is a separate question from these obligations. Certification, a self-assessment score, or the current state of the assessment program doesn't discharge the continuing safeguarding and reporting requirements in the contract, which

operate on their own terms. On the technical baseline, verify which revision of NIST SP 800-171 the contract requires, including any applicable class deviation, rather than assuming the newest publication automatically governs.

Conclusion

Discovering a spill is the beginning of the response, not the substance of it. The company that resolves one credibly is the company that preserved evidence before it deleted anything, reported on the facts it had within the time it had, coordinated with suppliers on evidence rather than assurances, verified its corrective actions, and wrote down both what it established and what it couldn't. The difference between the two responses in this paper wasn't budget, tooling, or sophistication. It was whether the company treated an ordinary Monday morning email as the incident it was, and whether the record it built could carry the weight that would later be placed on it.

About the Author

David W. Koran holds the CyberAB Registered Practitioner Advanced (RPA) credential and is the founder of a consulting practice serving Defense Industrial Base contractors and their legal counsel, focused on readiness, enablement, and implementation. He is an Associate Member of the ABA Section of Public Contract Law and the author of *The CMMC Decision*. He can be reached at dkoran@davidkoran.com and (802) 335-2662.

References

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, acquisition.gov.

DFARS PGI 204.7303-3, Cyber Incident and Compromise Reporting, acquisition.gov.

DoD Cyber Crime Center (DC3), DIB Cybersecurity: Cyber Incident Reporting and Support Resources, dc3.mil.

32 CFR Part 2002, Controlled Unclassified Information, eCFR.

National Archives and Records Administration, CUI Registry, archives.gov.

NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, csrc.nist.gov.

NIST SP 800-88 Rev. 2, Guidelines for Media Sanitization, csrc.nist.gov.

NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, csrc.nist.gov.

Bureau of Industry and Security, BIS Imposes $2.77 Million Penalty on 3D Printing Company for Exports to China and Germany, Including Aerospace and Military Design Documents, February 27, 2023, bis.gov.

DoD Office of Inspector General, DODIG-2019-105, Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems, July 2019, dodig.mil.

U.S. Department of Justice, Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations, March 26, 2025, justice.gov.

U.S. Department of Justice, Honeywell Aerospace Inc. Agrees to Pay Over $2M to Settle False Claims Act Allegations of Failing to Comply with Cybersecurity Requirements in a U.S. Department of Defense Contract, September 1, 2026, justice.gov.

Center for Development of Security Excellence, Unauthorized Disclosure of Classified Information and Controlled Unclassified Information Student Guide, January 2025, cdse.edu.