BRAZEN LEARNING

DIB-IR: Total Federal Incident Response & Compliance Engine

A local-first, offline-capable incident structuring workspace for DFARS 252.204-7012, CMMC 2.0, and related federal incident-response and reporting obligations. Nothing you enter ever leaves this browser tab.

System Boundary & Data Custody Notice

This tool operates exclusively as an unauthenticated, local-browser sandbox for incident structuring and tabletop preparation. It is not an authorized System of Record, nor is it a certified compliance reporting system.

Data Isolation: Exposing actual FCI/CUI data to an unauthorized system environment can constitute a security incident or compliance gap. Users are strictly responsible for ensuring no live, protected data is entered outside their organization's authorized system security boundary.

Regulatory Obligations: Utilization of this interface does not satisfy, replace, or modify your organization's formal Incident Response Plan, outside counsel protocols, or mandatory federal reporting obligations (e.g., DC3/DCISE).

Review the full liability disclaimer and terms of use at the base of this page.

Why This Tool Is Single-User

A deliberate security decision, not a limitation we plan to fix.

This tool does not support multiple people editing the same incident at once. The moment two people need to work an incident from two different devices in real time, the data has to leave this browser and pass through some server or sync layer — and that breaks the core promise of this tool, which is that FCI/CUI incident data never leaves your local machine.

Instead: one owner works an incident at a time. Use the **Print / Save as PDF** option on any report to share a point-in-time snapshot with counsel, comms, or leadership. And when you're done, use the **DEFCON-1 PURGE** button below to wipe the workspace completely — no lingering copy of sensitive incident data is left sitting in a browser profile.

Engine Status

⚠ DEFCON-1 PURGE

Regulatory reference data and scenario library loaded for this session.

110	15	14	2
NIST 800-171 CONTROLS	CMMC L1 REQUIREMENTS	TABLETOP SCENARIOS	SAVED INCIDENTS

Saved Incidents

Every incident is encrypted and persisted locally as you work — reopen one here at any time, including after a refresh.

Live Incident — 7/18/2026
Live · Discovered 7/18/2026, 8:07:16 PM
OPEN Resume Delete

Live Incident — 7/18/2026
Live · Discovered 7/18/2026, 7:58:03 PM
OPEN Resume Delete

Subcontractor Roster

Save each subcontractor's contact info once here, then add them into any incident's flow-down matrix with one click instead of retyping.

Subcontractor name | Contact email/phone | CAGE code (optic | Notify hours (24)

Add

No subcontractors saved yet.

IR Exercise Completion Log

Every tabletop exercise you complete is logged here as evidence your organization tests its incident response capability (NIST SP 800-171 3.6.3).

No completed exercises yet. Run a tabletop scenario through to its final stage to log one.

Export Completion Log

Organization Profile

Sets your flow-down role for every incident you open. You can change this per-incident later.

Your role in the supply chain

Prime Contractor | Subcontractor

Does your organization hold a Facility Clearance (FCL)?

Toggling this on surfaces NISPOM / ICD 503 classified-network reporting requirements alongside the unclassified CUI workflow.

Yes — Cleared Facility | No — Uncleared

Save Organization Profile

Select a Mode

Tabletop Exercise is the recommended way to use this tool for course practice. Live Tracking is a working demonstration of the same engine against a real timeline.

RECOMMENDED

Tabletop Exercise Simulator

Run one of 14 hardcoded, hyper-detailed defense-contractor scenarios. Mid-exercise injects (regulatory, legal, operational, PR) fire as you progress. Nothing here is a real incident.

USE WITH CAUTION

Live Incident Tracking

Starts a real 72-hour DFARS clock against data you enter yourself. Read the disclaimer banner above before using this for anything but a drill.

[LIVE] Live Incident — 7/18/2026

Reminder: this starts a real countdown against whatever you enter below. See the disclaimer banner at the top of the page.

Classify the data involved (DFARS 252.204-7012)

This drives which reporting clock and control families apply. Select every category that is confirmed or suspected — do not wait for full certainty to start the clock.

Controlled Technical Information (CTI) | Critical Program Information (CPI) | Naval Nuclear Propulsion Info (NNPI) | Other CDI / CUI | FCI Only (No CUI Confirmed)

Cloud Service Provider involved?

Yes | No

Start 72-Hour Clock & Evaluate Triggers

02:23:24:09

REMAINING TO DC3/DCISE REPORT (72 HOURS FROM DISCOVERY)

90-day media/forensic preservation deadline: 10/16/2026, 8:07:16 PM

Applicable Regulatory Triggers

`DFARS-7012-CDI · DFARS Part 204`

DFARS 252.204-7012 — Cyber Incident Reporting

CDI/CUI (including CTI, CPI, or NNPI) was involved or reasonably suspected. The 72-hour DC3/DCISE reporting clock starts at the moment of discovery, and the 90-day media preservation obligation attaches immediately.
Why: Data classification includes CTI, CPI, NNPI, CDI — this is CDI/CUI under DFARS 252.204-7012.

`FAR-52.204-21 · FAR Part 4`

FAR 52.204-21 — Basic Safeguarding (FCI)

Federal Contract Information was involved. The 15 basic safeguarding requirements apply regardless of whether CUI is also present.
Why: Every federal contract touching Federal Contract Information carries the FAR 52.204-21 baseline, independent of the CUI-specific clauses above.

`CMMC-L2 · 32 CFR Part 170`

CMMC Level 2 — NIST SP 800-171 Assessment Impact

A confirmed CUI incident is evidence relevant to your current NIST SP 800-171 self-assessment score in SPRS. Depending on which controls failed, this may require a POA&M entry or, for controls that cannot carry a POA&M, an immediate score adjustment. Status check: DoD suspended CMMC Phase 2 (third-party/C3PAO certification) on July 13, 2026 pending a 60-day program review — the self-assessment obligations discussed

here are Phase 1 and remain unaffected. Confirm current CMMC program status before assuming anything about third-party certification requirements.
Why: CUI was involved, which places this incident squarely inside your CMMC Level 2 assessment boundary.

NNPI-SPECIAL · DFARS Part 204 / NAVSEA S9AA0-AA-GYD-010

NNPI — Naval Nuclear Propulsion Information Handling

NNPI carries handling and reporting requirements layered on top of standard CDI rules, generally routed through NAVSEA / the Naval Nuclear Propulsion Program in addition to DC3/DCISE.
Why: You flagged Naval Nuclear Propulsion Information as involved — route this to your NNPI point of contact immediately in parallel with DC3/DCISE reporting.

CPI-AT · DoDI 5200.39

CPI — Critical Program Information / Anti-Tamper

Critical Program Information incidents often carry Anti-Tamper and technology-protection plan reporting obligations to the program office in addition to DC3/DCISE.
Why: You flagged Critical Program Information — notify your program office's security manager alongside the standard DC3/DCISE report.

CSP-7012-b2 · DFARS Part 204

DFARS 252.204-7012(b)(2)(ii)(D) — Cloud Service Provider Check

When CDI is processed, stored, or transmitted through a cloud service provider on your behalf, that CSP must meet security requirements equivalent to FedRAMP Moderate baseline and must be capable of supporting your cyber incident reporting obligations, including providing you access to the incident data needed to report within 72 hours.
Why: A cloud service provider is involved and CUI is present — confirm the CSP's FedRAMP Moderate equivalence determination and incident-support flow-down clause before you rely on their data for your DC3/DCISE submission.

SPRS-7024 · DFARS Part 204

DFARS 252.204-7024 — SPRS Risk Profile Impact

Cyber incidents and any resulting control deficiencies feed into how your organization is viewed in the Supplier Performance Risk System, which contracting officers may weigh in future source selection decisions.
Why: A CUI incident with any confirmed control failures is exactly the kind of event that can affect how your SPRS risk profile reads to a future source-selection official.

Auto-Isolated NIST SP 800-171 Control Families

Based on your classification, these families are flagged for immediate review under CMMC Level 2. Built on Rev 2 (still the current CMMC baseline as of July 2026) — DoD has signaled a Revision 3 transition via future rulemaking, estimated late 2026–2027. Confirm current status before relying on Rev 2 control numbers.

AC — Access Control ⚠ | AT — Awareness & Training | AU — Audit & Accountability | CM — Configuration Management ⚠ | IA — Identification & Authentication | IR — Incident Response ⚠ | MA — Maintenance | MP — Media Protection ⚠

PS — Personnel Security | PE — Physical Protection | RA — Risk Assessment | CA — Security Assessment | SC — System & Communications Protection ⚠ | SI — System & Information Integrity ⚠

Immutable-Evidence Timeline Log

Hash-chained, append-only. Each entry is tamper-evident (any edit breaks the chain) — this is not literal write-once storage, so treat it as a defensible audit trail, not a substitute for real forensic custody procedures.

2026-07-19T01:07:16.330Z	Incident discovered — 72-hour clock started	f4650399…
2026-07-19T01:07:16.346Z	Data classification committed	eb5170c1…

Verify Chain Integrity

Media Preservation & Evidence Checklist

The 90-day forensic image / packet capture retention rule under DFARS 252.204-7012(d). Each check is logged with a timestamp; unchecking logs a reversal — this list cannot be silently edited.

Forensic image of affected system(s) captured

Done | N/A

Use a hardware write-blocker and your organization's approved imaging tool (e.g., FTK Imager, dd/dcfldd) to create a bit-for-bit image of every affected storage device before any further analysis touches the original media. Work from the image afterward, never the original.

Notes — system identifiers, hash values, serial numbers, file/log locations…

Network packet capture (PCAP) preserved for the incident window

Done | N/A

Pull PCAP from whatever is already capturing your traffic — a SPAN/mirror port, an IDS/IPS platform (e.g., Zeek, Suricata), or a firewall's packet-capture feature — covering the incident time window. If nothing was capturing traffic at the time, mark this Not Applicable rather than leaving it open.

Notes — system identifiers, hash values, serial numbers, file/log locations…

Volatile memory (RAM) captured before any system power-down

Done | N/A

Capture RAM before powering down or rebooting any affected system, using an approved memory-acquisition tool (e.g., FTK Imager, Magnet RAM Capture, WinPmem). If the system was already powered off before your team could respond, that window is gone — mark Not Applicable and note why rather than leaving it unresolved.

Notes — system identifiers, hash values, serial numbers, file/log locations...

Cryptographic (SHA-256) hash log started for all preserved images/files Done N/A

Use the SHA-256 hasher in the DC3 workflow section below (or your organization's standard forensic tool) to hash every preserved image and file the moment it's captured, before any further handling. Log the filename and hash value in the notes field for each item.

Notes — system identifiers, hash values, serial numbers, file/log locations...

Chain-of-custody log opened for all preserved evidence Done N/A

Open a chain-of-custody record for every piece of preserved evidence: who collected it, exactly when, where it's stored, and every person who has handled it since. Use your organization's standard chain-of-custody form or log system — reference where that log lives in the notes field.

Notes — system identifiers, hash values, serial numbers, file/log locations...

90-day retention calendar reminder created Done N/A

Set a calendar reminder for 90 days from the date of discovery (the countdown clock above shows the exact date) with whoever owns evidence retention at your organization, so preserved media isn't released or overwritten before DoD's window to request it closes.

Notes — system identifiers, hash values, serial numbers, file/log locations...

DC3 Malware Isolation Workflow

Guidance only — always follow your own IR plan and current DC3 submission instructions at dc3.mil.

1. Do NOT power off the affected system — powering off destroys volatile RAM evidence. If you must isolate, pull the network connection (or apply a host-based network block) rather than powering down.
2. Capture volatile memory (RAM) first, before disk imaging, using your organization's approved forensic RAM-capture tool.
3. Create a full forensic disk image using a write-blocker; work from the image going forward, never the original media.

4. Identify and isolate suspected malicious files; compute a SHA-256 hash of each one before any further handling (use the hasher below).

5. Stage hashed malware samples on read-only or air-gapped media — never re-execute suspected malware on a network-connected host.

6. Package the malware sample, its SHA-256 hash, and a brief technical summary for DC3 submission per current DC3 malware submission instructions (verify the current submission process at dc3.mil — intake procedures change).

7. Document every step above with timestamps in your chain-of-custody log.

SHA-256 File Hasher (runs entirely in this browser — the file is never uploaded anywhere)

Choose File No file chosen

Logged Malware Hashes

No hashes logged yet.

Tactical Communications & Privilege

When to go out-of-band: As soon as insider threat, business email compromise, or logging-integrity concerns are suspected — the corporate email/chat system itself may be compromised or monitored by the threat actor.

Preserving attorney-client privilege: Engage outside counsel early and have counsel (or someone directed by counsel) commission the forensic investigation. Mark investigative work product 'Attorney-Client Privileged / Prepared at the Direction of Counsel,' route findings through counsel, and keep the distribution list limited to a need-to-know IR core team.

Separate legal from technical work product: Purely technical remediation steps (patching, rebuilding a server) are generally not privileged. Legal-risk assessments and investigative findings commissioned by counsel may be. Avoid mixing the two in the same document.

Verify identity out-of-band: During an active compromise, verify participant identity through a second channel before sharing sensitive findings — impersonation of IR team members is a known attacker technique during live incidents.

- [ ] Out-of-band channel (e.g., Signal, isolated conferencing) established for this incident
- [ ] Outside counsel engaged and directing privileged workstreams

- [ ] IR core team distribution list limited to need-to-know participants

Subcontractor / Prime Flow-Down Matrix

Prime flow-down: add every subcontractor whose CDI/CUI may be affected. Each needs formal notice of their own DFARS 252.204-7012 obligations (implement NIST SP 800-171, report incidents affecting CDI on this subcontract to you and via DC3/DCISE, and provide you their DC3/DCISE report number).

Or add a one-off subcontractor not in your roster

Subcontractor name | Contact email/phone | Add

No subcontractors added yet.

DC3/DCISE Reporting Wizard

Important: the DIBNet portal was decommissioned June 6, 2025. Cyber incident reporting under DFARS 252.204-7012 now runs through DC3's DIB Collaborative Information Sharing Environment (DCISE) at icf.dcise.cert.org (same DoD-approved medium assurance certificate requirement as before), generating an XML file you submit via encrypted email, the DoD SAFE platform, or directly to dcise@us.af.mil. DFARS 252.204-7012(c) itself still doesn't enumerate the required fields — it just points to "the required elements" on that authenticated portal, which this app cannot access or verify against. The fields below reflect how this requirement is commonly implemented in practice, not the current DCISE form. Use this to organize your facts before you file — the DCISE process is the only authoritative source for exact current field requirements, and your actual filing happens there, not here.

REPORTING ENTITY

Company Name

Facility CAGE Code

DUNS / Unique Entity ID (UEI)

Point of Contact — Name

Point of Contact — Phone

Point of Contact — Email

CONTRACT INFO

Contract Number(s) or Agreement(s) Affected

Contracting Officer — Name / Contact

USG Program Manager — Name / Contact (if known)

DoD Programs, Platforms, or Systems Involved

Facility Clearance Level

— Select —

INCIDENT DETAILS

Location(s) of Compromise

Type of Compromise

— Select —

Impact to Covered Defense Information

Ability to Provide Operationally Critical Support Affected?

— Select —

TECHNICAL NARRATIVE

Description of Technique / Method Used

Incident Outcome

— Select —

Malware Involved?

— Select —

Incident/Compromise Narrative Summary

Additional Information / POC

Generate DC3/DCISE Submission Text

Resolve Incident

Mark Incident Resolved

Generate Reports

These files are not encrypted or password-protected when saved. After downloading or printing to PDF, password-protect or encrypt the file yourself (e.g., in Adobe Acrobat) before sharing it with anyone.

Technical Forensic Log

Timeline, hashes, affected systems

Download .md Print / PDF

Executive & SPRS Risk Briefing

Business impact, POA&M, exposure

Federal Compliance Docket

72-hr timeline proof, DC3/DCISE fields

Download .md Print / PDF

Download .md Print / PDF

Workspace Controls

Export Workspace (Encrypted)

Import Workspace

Lock Workspace