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	0
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.

No incidents saved yet. Start a tabletop scenario or a live incident below — it will appear here as soon as you commit a data classification.

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.

Tabletop Scenario Library

Select a scenario to view its briefing and open a tracked practice incident. (Stage-by-stage inject delivery ships in the next build phase — for now this loads the full scenario briefing, initial classification, and starts the countdown clock exactly as a real incident would.)

SC-01

Ransomware on Engineering Workstations

Ransomware / CUI Schematics

SC-02

Phishing-to-Exfiltration From a Cloud CUI Enclave

Credential Theft / Cloud

SC-03

Stolen Unencrypted Mobile Device

Physical Loss / FCI

SC-04

Malicious Insider — Mass CAD Exfiltration

Insider Threat

SC-05

Sub-Tier Vendor Total Network Breach

Supply Chain / Third Party

SC-06

Classified-to-Unclassified Data Spill

Classified Spillage

SC-07

Persistent Beaconing From a Compromised IoT Camera

IoT / Physical Facility

SC-08

Component Flagged by New FASCSA Exclusion Order

Supply Chain Exclusion

SC-09

DoS Attack on a DPAS-Rated Production Line

Availability / Priority Contract

SC-10

Whistleblower Reports Systemic MFA Failure

Self-Disclosure / Insider Report

SC-11

Business Email Compromise / Vendor Payment Fraud

Financial Fraud / BEC

SC-12

Software Supply Chain / SBOM Compromise

Supply Chain / Software

SC-13

M&A / Novation Legacy Compliance Gap

M&A / Contract Novation

SC-14

False Positive / Non-Reportable Alert

Non-Incident / Documentation

[TABLETOP] Ransomware on Engineering Workstations

At 6:40 AM, your engineering team's shared CAD file server stops responding. By 7:15 AM, three engineers report their workstations are displaying a ransom note. Initial triage shows the encrypted share contained proprietary CUI-marked schematics for a subsystem under a current DoD development contract, including drawings bearing 'CTI' distribution statements. Backups exist but the last verified-clean backup is six days old.

Scenario Progress

1 2 3

Begin Stage 1

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

Workspace Controls

Export Workspace (Encrypted) Import Workspace Lock Workspace