Navigating DFIR in the Defense Industrial Base

Strategic Alignment of DFARS 7012, CMMC, 32 CFR,
and Cyber Insurance Architectures

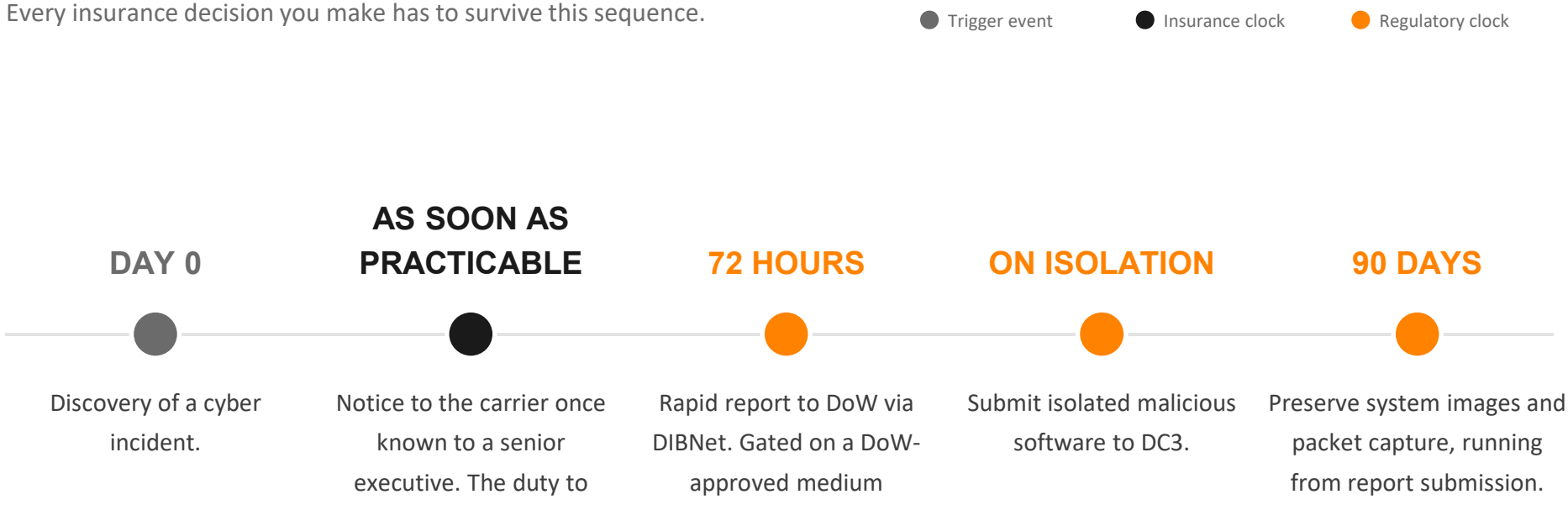
Rick Rosenberry

Cyber Insurance Wholesaler · GovCon Risk Advisor

rick.rosenberry@ukon.com

The Clock You're Insuring Against

Every insurance decision you make has to survive this sequence.



Two clocks, one incident. If the panel process starts on day two, you are already inside the 72-hour window.

UKON

The Panel Conflict

Notice triggers a duty to cooperate. Cooperation means using their vendors.

WHAT YOUR POLICY REQUIRES

- Notice as soon as practicable once the incident is known to a senior executive.
- A contractual duty to cooperate with the carrier.
- Counsel, DFIR, and crisis communications drawn from the carrier's approved panel.
- Going off panel without consent can put reimbursement of those response costs at risk.

WHAT DIB Contractors Need

- DFIR professionals who understand CUI handling guidelines.
- Legal team that understands DFARS 7012, 32 CFR and 22 CFR.
- U.S. persons on U.S. soil where ITAR or NOFORN applies. All us servers.
- Reporting and evidence handling aligned to DFARS 252.204-7012.

UKON

The Scoping Trap

The exemption that protects you is the exemption your responders can void.

01

OUT OF SCOPE

A provider needing only temporary access for incident response or forensics is not an ESP and is not deemed to handle CUI. Their lab is not a Security Protection Asset.

02

THE HARVEST

Automated triage collects indiscriminately: the Master File Table, Windows event logs, volatile RAM. Nobody reviews it first. That is the point of triage.

03

IN SCOPE

CUI rides out inside filenames, command-line strings, and document fragments. The temporary-access position collapses and their infrastructure enters your boundary.

Temporary-access language: CMMC Final Rule preamble, 89 FR 83092 (Oct. 15, 2024). Preamble commentary, not the text of 32 CFR 170.19.

UKON

Provisional Access Architecture

How to let a non-certified DFIR firm work without expanding your scope.

01 **HARDEN THE VDI**

Block clipboard redirection, local drive mapping, printing, and screen capture.

02 **CONTROL INGRESS**

Pre-staged, malware-scanned tool share. Allowlist only trusted repositories.

03 **SEGMENT IT**

Routes to your SIEM and EDR consoles only. Isolate from CUI repositories.

04 **GATE IDENTITY**

Phishing-resistant MFA, plus login restricted to the firm's egress IPs.

05 **SIZE FOR FORENSICS**

8 to 16 vCPU, 32GB+ RAM, premium SSD. A standard profile will crawl.

06 **VET THE HUMANS**

Written U.S.-person confirmation. MSA clause for incidental CUI contact.

UKON

Before You Bind

Everything above is cheap to fix today and expensive to fix at 2 a.m.

01 Name your vendors.

Legal, DFIR, and crisis communications firms that already work in the DIB and understand CUI handling.

02 Get them on the panel before inception.

Not at renewal. Not after the incident. Carriers will add vendors, but only while you still have leverage.

03 Document the coordination plan.

Written, pre-incident, and specific about who calls whom in the first four hours.

Rick Rosenberry

Cyber Insurance Wholesaler · GovCon Risk Advisor · rick@ukon.com

Full white paper available. Email me.

UKON