WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Sunday, 22 November 2026 | Vol. 2026-326 | As of 220730 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, trend ↑, as reported intrusions into two federal systems add to an already heavy week. People briefed on the case told CNN and AP that the FBI is investigating an apparent hack of its National Crime Information Center. The FBI has not confirmed it. A USDA internal email seen by Nextgov/FCW confirms a "security incident" that forced password resets and took farm-payment applications offline. Monadnock Community Hospital is on day 14 of ambulance diversion. Ransomware.live counts 391 leak-site victims for 16–22 Nov, 45% above the 8-week mean. On chips, Samsung told Korean media it has "no cases" of halted shipments to Chinese customers. MOFCOM has named no countermeasure, and No. 72 lapses on 27 Nov. It is Sunday: no KEV update, Federal Register rule or MOFCOM notice has appeared since Friday. No calls are due. New: TEC-57, TEC-58.

0. WIRE Technology & Cyber Dashboard

TOPIC	CRISIS LEVEL	DOM. INDICATOR	KEY DRIVER (today)	TREND
TEC-T1 Critical-infrastructure cyber	ENVIRONMENT FOR CRISIS	SIGNIFICANT	K-3: Monadnock diversion day 14; reported NCIC and USDA intrusions; K-4: 391 victims (+45%)	↑
TEC-T2 Semiconductors and compute	ENVIRONMENT FOR CRISIS	SIGNIFICANT	X-1: BIS rule in force, Samsung denies halts; X-2: No. 72 lapses 27 Nov, no notice	=
TEC-T4 AI governance and incidents	ENVIRONMENT FOR CRISIS	SIGNIFICANT	AI-2: OpenRouter off-boards 3 inference providers after Dragos canary study	=
TEC-T3 Space and undersea infrastructure	NO CRISIS	ABNORMAL	O-2: Gulf of Finland GNSS interference 45% of area-hours on 21 Nov; SMW5 fault off Pakistan, cause unknown	=

Indicator: ROUTINE ABNORMAL SIGNIFICANT EXTREME **Crisis level:** NO CRISIS ENV. FOR CRISIS POTENTIAL PROBABLE IMMINENT

Family level = highest topic level. Roll-up per WIRE_METHOD §1a. Trend key: ↑ toward crisis, ↓ away, = no net change.

Change line. No topic changes level, and the family trend stays ↑ because of TEC-T1.

Moved indicators (vs 21 November). No indicator changed its score. K-4 rose from 367 to 391 victims and stays ABNORMAL. O-2 readings rose to 45% of area-hours, from 16–19% on weekdays, and the score stays ABNORMAL. K-1 is unchanged at 9, because CISA published no catalog update on 21–22 Nov.

I. TEC-T1 CRITICAL-INFRASTRUCTURE CYBER | ENVIRONMENT FOR CRISIS

Facts. The KEV feed is still at version 2026.11.20 with 1,790 entries. It holds 9 additions dated 16–22 Nov (KEV feed; GitHub mirror). The federal deadline for vCenter flaw CVE-2026-123890 and three other entries is 23 Nov. CISA has made no attribution (CISA KEV). GTIG's 19 Nov report says suspected PRC-nexus actor ARMORY CASTLE exploited the flaw in early September (GTIG). CISA's directives page lists no new Emergency Directive; the latest is still ED 26-03 (CISA directives). Two people briefed on the probe told CNN that the FBI is investigating an apparent intrusion into NCIC, and AP has a source saying the same. The FBI has not confirmed the intrusion. It is unclear when it happened or whether data was taken (AP; BleepingComputer). At USDA, the Cybersecurity and Privacy Operations Center "uncovered a security incident", according to a 16 Nov internal email seen by Nextgov/FCW. The incident forced a reset of all database passwords and caused outages in farm-payment tools. Nobody has said who did it or whether data was exfiltrated (Nextgov/FCW; NBC). Monadnock Community Hospital's 20 Nov update still reports ambulance diversion. Lab, radiology and some major elective surgeries are cancelled through 30 Nov, and the next update is promised "early next week" (MCH). Ransomware.live counts 109, 59, 69, 74, 49, 25 and 6 victims for 16–22 Nov (UTC, with 22 Nov partial). The total of 391 compares with an 8-week mean of 269.5 (feed). No Monadnock entry appears. EDGAR full-text search for 19–22 Nov returns only an iQSTEL 8-K. It was filed under Item 8.01, not 1.05 (EDGAR FTS). **Indicators.** K-1 ROUTINE (9); K-2 ABNORMAL (carried; no official state attribution); K-3 SIGNIFICANT (Monadnock); K-4 ABNORMAL (+45%); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend ↑. **Analyst Comment.** NCIC and USDA are federal systems rather than critical infrastructure in the strict sense, so they do not move K-3 today. NCIC matters because police use it during street checks, so integrity damage would hurt operations quickly. An FBI confirmation would firm this up (logged as TEC-57: 45%). TEC-43 (≥ 10 KEV additions) needs a catalog update dated 22 Nov. None has appeared, so the call is very likely to miss when it is checked tomorrow.

II. TEC-T2 SEMICONDUCTORS AND COMPUTE | ENVIRONMENT FOR CRISIS

Facts. The Federal Register's public-inspection list for 23 Nov carries only a BIS information-collection notice and no new rule (FR PI). Responding to the FT report, Samsung Electronics said there are "currently no cases of shipments halted to Chinese customers" (Dong-A Ilbo, 20 Nov). TSMC said it would not comment on "market rumours" and would comply with the BIS rule where it applies (same source). MOFCOM's only statement remains the 17 Nov spokesperson answer threatening countermeasures (MOFCOM). Independent trackers checked on 21 and 22 Nov found no notice extending No. 72 past 27 Nov (CRUCIBEL; TIMEWELL; MOFCOM No. 72). **Indicators.** X-1 SIGNIFICANT; X-2 ABNORMAL; X-3 ROUTINE (carried); X-4 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** Samsung's denial weakens TEC-56 (on-record confirmation of a pause), which now looks about 15% likely. The ledger value is unchanged.

III. TEC-T4 AI GOVERNANCE AND INCIDENTS | ENVIRONMENT FOR CRISIS

Facts. On 22 Nov OpenRouter said it had off-boarded three inference providers and removed 125 endpoints from Zero Data Retention eligibility. It acted after security researchers found that some providers' data had been compromised or that their data policies were not being honoured. OpenRouter says it was not breached itself, and it links notices from Novita, Phala and Together (OpenRouter). The researchers were at Dragos. They sent nearly two million prompts seeded with trackable secrets and found evidence that attackers had compromised at least three AI providers and siphoned the prompts those providers received (Ars Technica). No new AI-specific federal action appears in the Federal Register for 20–23 Nov (FR API). **Indicators.** AI-1 ABNORMAL (carried); AI-2 ABNORMAL (provider data exposure, no service disruption); AI-3 SIGNIFICANT (carried). Roll-up: ENVIRONMENT FOR CRISIS. Trend =.

IV. TEC-T3 SPACE AND UNDERSEA INFRASTRUCTURE | NO CRISIS

Facts. GNSS interference over the Gulf of Finland and Estonia hit its 30-day high on 21 Nov, at 45% of 163 area-hours. The figure for 22 Nov so far is 41% of 49 area-hours (NAVWAR monitor). Pakistan's regulator reported a fault in the SEA-ME-WE 5 cable about 11 km offshore. No cause has been given, and the operator expects repairs by 6 Dec (Dawn). No new attributed sabotage was found. **Indicators.** O-1/O-2/O-3 ABNORMAL (carried). **Override −1 to NO CRISIS (held):** the only sabotage event in the 30-day window failed. Trend =.

V. PREDICTIONS

Resolved: none. No open TEC call has passed its resolve-by date. TEC-42 was already resolved as a miss on 20 Nov. **Pending:** TEC-43 (9 of 10; checked 23 Nov; very likely miss). TEC-44 (391 of 330; checked 24 Nov; very likely hit). TEC-52 (Monadnock diversion lifted by 25 Nov; unlikely). TEC-09 (No. 72 extension; 27 Nov). TEC-07 (Emergency Directive; 30 Nov). TEC-51 (MOFCOM countermeasure; 18 Dec). TEC-56 (Samsung confirmation; 15 Dec; weakened). **New:** - **TEC-57:** The FBI confirms on the record an intrusion or cybersecurity incident affecting NCIC by 6 Dec 2026. **45%, about even.** - **TEC-58:** Monadnock Community Hospital says it has resumed outpatient laboratory or radiology services by 1 Dec 2026. **35%, unlikely.**

VI. GAPS AND UNVERIFIED

- NCIC: the reports rest only on unnamed sources (CNN, AP). There is no FBI confirmation, timeline, actor or data impact.
- USDA: there is no public USDA statement, and the actor and any exfiltration are unknown. NBC's account rests on former officials.
- vCenter attribution remains vendor-only (GTIG/Mandiant).
- An IT Sicherheitsnews item dated 21 Nov says Greiz hospital is not taking emergencies. MDR reported on 16 Nov that the emergency department had reopened. The current status is not confirmed.
- SMW5: the cause is unknown, and nothing suggests sabotage.
- Samsung's denial comes from Korean press (Dong-A) and is not on Samsung's own newsroom.

Sources

CISA; CISA KEV (feed and GitHub mirror); Google Threat Intelligence Group; AP; BleepingComputer; Nextgov/FCW; NBC News; Monadnock Community Hospital; ransomware.live; SEC EDGAR; Federal Register; Dong-A Ilbo; MOFCOM; CRUCIBEL; TIMEWELL; OpenRouter; Ars Technica; NAVWAR RFI monitor; Dawn.