Reference Availability Report

Footnoted and Verified Source Material — Availability Index

Eleanor Vance / AI Cyber Security Research Boardroom

2026-05-31

Contents

Chapter 1

Reference Availability Report

Document ID: AICSR-REF-INDEX-2026-001
Generated: 2026-05-31
Total references: 38
Available: 38 | **Partial:** 0 | **Unavailable:** 0

This index catalogs every footnoted and verification-ledger reference used in the boardroom study corpus. Each reference has a dedicated article file in `output/references/articles/` (Markdown, LaTeX, and PDF).

1.1 Summary

Status	Count	Meaning
available	38	Full or substantial text captured in article file
partial	0	Source reached but text extraction incomplete (paywall shell, PDF scan, JS-rendered page)
unavailable	0	Automated retrieval blocked or local file missing
fallback_recovered	4	Primary blocked; content captured via alternate mirror documented in Capture Provenance

1.2 Fallback Recovery Methods

Hard-to-capture references use ordered fallback strategies documented in this report and `REFERENCE-MANIFEST.yaml`:

Key	Primary blocker	Fallback method
`mitre-atlas`	JS-rendered SPA	GitHub YAML mirror (`mitre-atlas/atlas-data`)
`njccic-house`	Imperva Incapsula WAF	Corroborating encyclopedia (Wikipedia / FT citation)
`gao-classified`	gao.gov HTTP 403	Corroborating press (Bloomberg Government summary)
`gao-water`	gao.gov HTTP 403	Corroborating press (Route Fifty summary)
`sigstore-cosign`	Legacy URL 404	Current docs path `/cosign/`

To refresh only hard-to-capture references, update the article Markdown for keys in the fallback table below and rebuild their PDF siblings.

1.3 Available References

- **`abs-ref`** — Boardroom Comprehensive Abstracts AICSR-ABS-2026-001
  - Article: `output/references/articles/abs-ref.pdf`
  - Source: output/Boardroom-Comprehensive-Abstracts.md
- **`bgov-gao`** — Bloomberg Government — 815 classified data violations summary
  - Article: `output/references/articles/bgov-gao.pdf`
  - Source: https://news.bgov.com/bloomberg-government-news/us-companies-had-815-classified-data-violations-gao-finds
- **`cisa-kev`** — CISA Known Exploited Vulnerabilities Catalog
  - Article: `output/references/articles/cisa-kev.pdf`
  - Source: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **`cisa-salt`** — CISA Advisory AA25-239A — Salt Typhoon
  - Article: `output/references/articles/cisa-salt.pdf`
  - Source: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a
- **`csa-cisa`** — CSA Research Note — CISA Leadership Governance Vacuum (2026-04-24)
  - Article: `output/references/articles/csa-cisa.pdf`
  - Source: https://labs.cloudsecurityalliance.org/research/csa-research-note-cisa-leadership-governance-vacuum-20260424/

- `csa-nvd` — CSA Whitepaper — NVD Infrastructure Crisis & AI Vulnerability Discovery
  - Article: `output/references/articles/csa-nvd.pdf`
  - Source: https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/05/CSA_whitepaper_NVD_inf csa-styled.pdf
- `dlg-ref` — Boardroom Complete Dialog Transcript AICSR-DLG-2026-001
  - Article: `output/references/articles/dlg-ref.pdf`
  - Source: output/Boardroom-Complete-Dialog-Transcript.md
- `eo-14409` — White House EO 14409 — AI Innovation and Security (2026-06-02)
  - Article: `output/references/articles/eo-14409.pdf`
  - Source: https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/
- `fbi-salt` — CyberScoop — FBI confirms Salt Typhoon still ongoing (Feb 2026)
  - Article: `output/references/articles/fbi-salt.pdf`
  - Source: https://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026/
- `gao-classified` — GAO-26-107861 — 815 Classified Contractor Security Violations
  - Article: `output/references/articles/gao-classified.pdf`
  - Source: https://www.gao.gov/products/gao-26-107861
  - **Recovered via:** `corroborating_press` from https://news.bgov.com/bloomberg-government-news/us-companies-had-815-classified-data-violations-gao-finds
- `gao-water` — GAO-26-109159 — Water Sector Cybersecurity
  - Article: `output/references/articles/gao-water.pdf`
  - Source: https://www.gao.gov/products/gao-26-109159
  - **Recovered via:** `corroborating_press` from https://www.route-fifty.com/cybersecurity/2026/02/gao-finds-gaps-water-sector-cybersecurity/402456/
- `gca-salt` — GCA — Salt Typhoon Across the Internet
  - Article: `output/references/articles/gca-salt.pdf`
  - Source: https://globalcyberalliance.org/new-report-salt-typhoon-across-the-internet/
- `gdpr-art32` — GDPR Article 32 — Security of processing
  - Article: `output/references/articles/gdpr-art32.pdf`

  - Source: https://gdpr-info.eu/art-32-gdpr/

- **horizon3-chain** — Horizon3.ai — LiteLLM chained with Starlette BadHost RCE
  - Article: `output/references/articles/horizon3-chain.pdf`
  - Source: https://horizon3.ai/attack-research/vulnerabilities/cve-2026-42271-chained-with-cve-2026-48710/

- **iec-62443** — ISA/IEC 62443 Industrial Cybersecurity Standards
  - Article: `output/references/articles/iec-62443.pdf`
  - Source: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

- **litellm-kev** — CISA Alert — CVE-2026-42271 LiteLLM added to KEV
  - Article: `output/references/articles/litellm-kev.pdf`
  - Source: https://www.cisa.gov/news-events/alerts/2026/06/08/cisa-adds-two-known-exploited-vulnerabilities-catalog

- **litellm-sqli** — The Hacker News — LiteLLM CVE-2026-42208 exploited within 36h
  - Article: `output/references/articles/litellm-sqli.pdf`
  - Source: https://thehackernews.com/2026/04/litellm-cve-2026-42208-sql-injection.html

- **matindex-ref** — Research Materials Index AICSR-MATINDEX-2026-001
  - Article: `output/references/articles/matindex-ref.pdf`
  - Source: output/RESEARCH-MATERIALS-INDEX.md

- **method-ref** — How the Research Was Done AICSR-METHOD-2026-001
  - Article: `output/references/articles/method-ref.pdf`
  - Source: output/How-The-Research-Was-Done.md

- **mit-ref** — MVAP Complete Mitigation Strategy AICSR-MIT-2026-001
  - Article: `output/references/articles/mit-ref.pdf`
  - Source: output/MVAP-Complete-Mitigation-Strategy.md

- **mitre-atlas** — MITRE ATLAS — Adversarial ML
  - Article: `output/references/articles/mitre-atlas.pdf`
  - Source: https://atlas.mitre.org/
  - **Recovered via:** `github_yaml_mirror` from https://raw.githubusercontent.com/mitre-

atlas/atlas-data/main/dist/v6/ATLAS-2026.05.yaml

- `mitre-t1059-001` — MITRE ATT&CK T1059.001 — PowerShell
  - Article: `output/references/articles/mitre-t1059-001.pdf`
  - Source: https://attack.mitre.org/techniques/T1059/001/
- `mitre-t1558-003` — MITRE ATT&CK T1558.003 — Kerberoasting
  - Article: `output/references/articles/mitre-t1558-003.pdf`
  - Source: https://attack.mitre.org/techniques/T1558/003/
- `ms-isac` — StateScoop — CISA ending MS-ISAC support
  - Article: `output/references/articles/ms-isac.pdf`
  - Source: https://statescoop.com/cisa-confirms-its-ending-ms-isac-support/
- `nist-airmf` — NIST AI Risk Management Framework 1.0
  - Article: `output/references/articles/nist-airmf.pdf`
  - Source: https://www.nist.gov/itl/ai-risk-management-framework
- `nist-genai` — NIST Generative AI Profile (NIST.AI.600-1)
  - Article: `output/references/articles/nist-genai.pdf`
  - Source: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
- `njccic-house` — NJCCIC — Salt Typhoon targets House Committee emails
  - Article: `output/references/articles/njccic-house.pdf`
  - Source: https://www.cyber.nj.gov/Home/Components/News/News/1935/214
  - **Recovered via:** `corroborating_encyclopedia` from https://en.wikipedia.org/wiki/Salt_Typhoon
- `ostif-badhost` — OSTIF — BadHost vulnerability in Starlette
  - Article: `output/references/articles/ostif-badhost.pdf`
  - Source: https://ostif.org/disclosing-the-badhost-vulnerability-in-starlette/
- `owasp-llm` — OWASP Top 10 for LLM Applications 2025
  - Article: `output/references/articles/owasp-llm.pdf`
  - Source: https://genai.owasp.org/llm-top-10/
- `owasp-llm01` — OWASP LLM01 — Prompt Injection
  - Article: `output/references/articles/owasp-llm01.pdf`

  - Source: https://genai.owasp.org/llmrisk/llm01-prompt-injection/

- `owasp-llm02` — OWASP LLM02 — Sensitive Information Disclosure
  - Article: `output/references/articles/owasp-llm02.pdf`
  - Source: https://genai.owasp.org/llmrisk/llm022025-sensitive-information-disclosure/

- `project-ref` — PROJECT.md — boardroom project metadata
  - Article: `output/references/articles/project-ref.pdf`
  - Source: PROJECT.md

- `sigstore-cosign` — Sigstore cosign — container/signing verification
  - Article: `output/references/articles/sigstore-cosign.pdf`
  - Source: https://docs.sigstore.dev/cosign/

- `slsa` — SLSA Supply-chain Levels for Software Artifacts v1.0
  - Article: `output/references/articles/slsa.pdf`
  - Source: https://slsa.dev/spec/v1.0/

- `study-ref` — AI Cyber Security Research Study AICSR-STUDY-2026-001
  - Article: `output/references/articles/study-ref.pdf`
  - Source: output/Cyber-Security-AI-Diligence-Research-Study.md

- `techcrunch-cisa` — TechCrunch — Acting CISA chief uploaded FOUO docs to ChatGPT
  - Article: `output/references/articles/techcrunch-cisa.pdf`
  - Source: https://techcrunch.com/2026/01/28/trumps-acting-cybersecurity-chief-uploaded-sensitive-government-docs-to-chatgpt/

- `trend-q1` — Trend Micro — U.S. Public Sector Under Siege Q1 2026
  - Article: `output/references/articles/trend-q1.pdf`
  - Source: https://www.trendmicro.com/en_us/research/26/d/us-public-sector-under-siege.html

- `vote-record-ref` — Formal Vote Record with dissent rationale
  - Article: `output/references/articles/vote-record-ref.pdf`
  - Source: sessions/VOTE-RECORD.md

1.4 Partially Available References

None.

1.5 Unavailable References

None.

1.6 Per-Article File Index

1.6.1 `abs-ref`

- **Title:** Boardroom Comprehensive Abstracts AICSR-ABS-2026-001
- **Status:** available
- **MD:** `articles/abs-ref.md`
- **PDF:** `articles/abs-ref.pdf`

1.6.2 `bgov-gao`

- **Title:** Bloomberg Government — 815 classified data violations summar
- **Status:** available
- **MD:** `articles/bgov-gao.md`
- **PDF:** `articles/bgov-gao.pdf`

1.6.3 `cisa-kev`

- **Title:** CISA Known Exploited Vulnerabilities Catalog
- **Status:** available
- **MD:** `articles/cisa-kev.md`
- **PDF:** `articles/cisa-kev.pdf`

1.6.4 `cisa-salt`

- **Title:** CISA Advisory AA25-239A — Salt Typhoon
- **Status:** available
- **MD:** `articles/cisa-salt.md`
- **PDF:** `articles/cisa-salt.pdf`

1.6.5 `csa-cisa`

- **Title:** CSA Research Note — CISA Leadership Governance Vacuum (2026-
- **Status:** available
- **MD:** `articles/csa-cisa.md`
- **PDF:** `articles/csa-cisa.pdf`

1.6.6 `csa-nvd`

- **Title:** CSA Whitepaper — NVD Infrastructure Crisis & AI Vulnerabilit

- **Status:** available
- **MD:** `articles/csa-nvd.md`
- **PDF:** `articles/csa-nvd.pdf`

1.6.7 `dlg-ref`

- **Title:** Boardroom Complete Dialog Transcript AICSR-DLG-2026-001
- **Status:** available
- **MD:** `articles/dlg-ref.md`
- **PDF:** `articles/dlg-ref.pdf`

1.6.8 `eo-14409`

- **Title:** White House EO 14409 — AI Innovation and Security (2026-06-0
- **Status:** available
- **MD:** `articles/eo-14409.md`
- **PDF:** `articles/eo-14409.pdf`

1.6.9 `fbi-salt`

- **Title:** CyberScoop — FBI confirms Salt Typhoon still ongoing (Feb 20
- **Status:** available
- **MD:** `articles/fbi-salt.md`
- **PDF:** `articles/fbi-salt.pdf`

1.6.10 `gao-classified`

- **Title:** GAO-26-107861 — 815 Classified Contractor Security Violation
- **Status:** available
- **MD:** `articles/gao-classified.md`
- **PDF:** `articles/gao-classified.pdf`

1.6.11 `gao-water`

- **Title:** GAO-26-109159 — Water Sector Cybersecurity
- **Status:** available
- **MD:** `articles/gao-water.md`
- **PDF:** `articles/gao-water.pdf`

1.6.12 `gca-salt`

- **Title:** GCA — Salt Typhoon Across the Internet
- **Status:** available
- **MD:** `articles/gca-salt.md`
- **PDF:** `articles/gca-salt.pdf`

1.6.13 `gdpr-art32`

- **Title:** GDPR Article 32 — Security of processing

- **Status:** available
- **MD:** `articles/gdpr-art32.md`
- **PDF:** `articles/gdpr-art32.pdf`

1.6.14 `horizon3-chain`

- **Title:** Horizon3.ai — LiteLLM chained with Starlette BadHost RCE
- **Status:** available
- **MD:** `articles/horizon3-chain.md`
- **PDF:** `articles/horizon3-chain.pdf`

1.6.15 `iec-62443`

- **Title:** ISA/IEC 62443 Industrial Cybersecurity Standards
- **Status:** available
- **MD:** `articles/iec-62443.md`
- **PDF:** `articles/iec-62443.pdf`

1.6.16 `litellm-kev`

- **Title:** CISA Alert — CVE-2026-42271 LiteLLM added to KEV
- **Status:** available
- **MD:** `articles/litellm-kev.md`
- **PDF:** `articles/litellm-kev.pdf`

1.6.17 `litellm-sqli`

- **Title:** The Hacker News — LiteLLM CVE-2026-42208 exploited within 36
- **Status:** available
- **MD:** `articles/litellm-sqli.md`
- **PDF:** `articles/litellm-sqli.pdf`

1.6.18 `matindex-ref`

- **Title:** Research Materials Index AICSR-MATINDEX-2026-001
- **Status:** available
- **MD:** `articles/matindex-ref.md`
- **PDF:** `articles/matindex-ref.pdf`

1.6.19 `method-ref`

- **Title:** How the Research Was Done AICSR-METHOD-2026-001
- **Status:** available
- **MD:** `articles/method-ref.md`
- **PDF:** `articles/method-ref.pdf`

1.6.20 `mit-ref`

- **Title:** MVAP Complete Mitigation Strategy AICSR-MIT-2026-001

- **Status:** available
- **MD:** `articles/mit-ref.md`
- **PDF:** `articles/mit-ref.pdf`

1.6.21 `mitre-atlas`

- **Title:** MITRE ATLAS — Adversarial ML
- **Status:** available
- **MD:** `articles/mitre-atlas.md`
- **PDF:** `articles/mitre-atlas.pdf`

1.6.22 `mitre-t1059-001`

- **Title:** MITRE ATT&CK T1059.001 — PowerShell
- **Status:** available
- **MD:** `articles/mitre-t1059-001.md`
- **PDF:** `articles/mitre-t1059-001.pdf`

1.6.23 `mitre-t1558-003`

- **Title:** MITRE ATT&CK T1558.003 — Kerberoasting
- **Status:** available
- **MD:** `articles/mitre-t1558-003.md`
- **PDF:** `articles/mitre-t1558-003.pdf`

1.6.24 `ms-isac`

- **Title:** StateScoop — CISA ending MS-ISAC support
- **Status:** available
- **MD:** `articles/ms-isac.md`
- **PDF:** `articles/ms-isac.pdf`

1.6.25 `nist-airmf`

- **Title:** NIST AI Risk Management Framework 1.0
- **Status:** available
- **MD:** `articles/nist-airmf.md`
- **PDF:** `articles/nist-airmf.pdf`

1.6.26 `nist-genai`

- **Title:** NIST Generative AI Profile (NIST.AI.600-1)
- **Status:** available
- **MD:** `articles/nist-genai.md`
- **PDF:** `articles/nist-genai.pdf`

1.6.27 `njccic-house`

- **Title:** NJCCIC — Salt Typhoon targets House Committee emails

- **Status:** available
- **MD:** `articles/njccic-house.md`
- **PDF:** `articles/njccic-house.pdf`

1.6.28 `ostif-badhost`

- **Title:** OSTIF — BadHost vulnerability in Starlette
- **Status:** available
- **MD:** `articles/ostif-badhost.md`
- **PDF:** `articles/ostif-badhost.pdf`

1.6.29 `owasp-llm`

- **Title:** OWASP Top 10 for LLM Applications 2025
- **Status:** available
- **MD:** `articles/owasp-llm.md`
- **PDF:** `articles/owasp-llm.pdf`

1.6.30 `owasp-llm01`

- **Title:** OWASP LLM01 — Prompt Injection
- **Status:** available
- **MD:** `articles/owasp-llm01.md`
- **PDF:** `articles/owasp-llm01.pdf`

1.6.31 `owasp-llm02`

- **Title:** OWASP LLM02 — Sensitive Information Disclosure
- **Status:** available
- **MD:** `articles/owasp-llm02.md`
- **PDF:** `articles/owasp-llm02.pdf`

1.6.32 `project-ref`

- **Title:** PROJECT.md — boardroom project metadata
- **Status:** available
- **MD:** `articles/project-ref.md`
- **PDF:** `articles/project-ref.pdf`

1.6.33 `sigstore-cosign`

- **Title:** Sigstore cosign — container/signing verification
- **Status:** available
- **MD:** `articles/sigstore-cosign.md`
- **PDF:** `articles/sigstore-cosign.pdf`

1.6.34 `slsa`

- **Title:** SLSA Supply-chain Levels for Software Artifacts v1.0

- **Status:** available
- **MD:** `articles/slsa.md`
- **PDF:** `articles/slsa.pdf`

1.6.35 `study-ref`

- **Title:** AI Cyber Security Research Study AICSR-STUDY-2026-001
- **Status:** available
- **MD:** `articles/study-ref.md`
- **PDF:** `articles/study-ref.pdf`

1.6.36 `techcrunch-cisa`

- **Title:** TechCrunch — Acting CISA chief uploaded FOUO docs to ChatGPT
- **Status:** available
- **MD:** `articles/techcrunch-cisa.md`
- **PDF:** `articles/techcrunch-cisa.pdf`

1.6.37 `trend-q1`

- **Title:** Trend Micro — U.S. Public Sector Under Siege Q1 2026
- **Status:** available
- **MD:** `articles/trend-q1.md`
- **PDF:** `articles/trend-q1.pdf`

1.6.38 `vote-record-ref`

- **Title:** Formal Vote Record with dissent rationale
- **Status:** available
- **MD:** `articles/vote-record-ref.md`
- **PDF:** `articles/vote-record-ref.pdf`

1.7 Regeneration

Edit reference article Markdown under `output/references/articles/`, update this availability report, and rebuild PDF and LaTeX siblings. See `output/references/CONTINUE-REFERENCES.md`.

Simulation note: External URLs reflect real published sources cited during the May 2026 boardroom simulation. Availability is measured at capture time and may change.