RELIABILITY FIRST

Agenda
Board of Directors

August 27, 2026 • 8:00 am – 1:00 pm (ET)

Inn Walden
1119 Aurora Hudson Rd
Aurora, OH 44202

Attire: Business Casual

Closed Agenda – Pyramid Room

Board of Directors – Executive Session

1. Confidential AI Strategy and Rollout Progress Update 8:00 am
Presenter: Atif Usman, Director Analytics and Risk

2. Confidential ERO Enterprise Artificial Intelligence Governance 8:30 am
Presenter: Marcus Noel, Vice President and CSO

3. Confidential Security Update 8:45 am
Presenter: Marcus Noel, Vice President and CSO

4. Confidential Executive Session 9:00 am
Presenter: Nelson Peeler, Chair

Open Agenda – Jodhpurs Lounge

1. Call to Order, Opening Remarks, and Appoint Secretary to Record Minutes 9:30 am
Presenter: Nelson Peeler, Chair

2. Antitrust Statement
Presenter: Niki Schaefer, Vice President and General Counsel
Reference: Antitrust Compliance Guidelines

3. Consent Items 9:35 am
Presenter: Nelson Peeler, Chair
Reference: *Minutes:*
a) Draft Minutes from April 30, 2026 Board Meeting
Resolutions:
a) Resolution to Hold Annual Meeting of Members (No. 2026-03)
Reference:
a) 2027 Board Meeting Dates
Action: Approve Consent Items

4. Data Center Activity 9:40 am

Presenter: Ohio House Representative Adam Holmes and Ohio Senator Brian Chavez
Description: Representative Adam Holmes, Chairman of the Ohio House Energy Committee, and Senator Brian Chavez, Chairman of the Senate Energy Committee, will discuss their joint legislative efforts to study and engage with data centers in Ohio through the Joint Data Center Committee.
Reference: None
Action: Information and Discussion

5. President's Report 10:15 am

Presenter: Tim Gallagher, President and CEO
Reference: None

6. E-ISAC Update on Artificial Intelligence 10:30 am

Presenter: Heather Lawrence, Sr. Data Scientist, E-ISAC
Reference: Ms. Lawrence will provide an update on artificial intelligence and its impact on reliability and security risks, including a discussion of how the E-ISAC is addressing those risks.
Reference: Presentation
Action: Information and Discussion

BREAK 11:00 am

Standing Updates (Information provided for transparency into key aspects of RF operations)

7. *Finance* 11:15 am

Christi Klein, Treasurer and Senior Manager Finance & Accounting, will provide a financial update.

8. *Security* 11:30 am

Jonathan Fischer, IT Manager, will provide an IT update relating to progress on stabilization, modernization, and transformation initiatives.

9. *Regulatory* 11:45 am

Diane Holder, Vice President Engineering and Strategic Engagement, will provide a regulatory update.

10. Data Center Landscape 12:00 pm

Presenter: Craig Sundstrom, Head of Energy & Sustainability Public Policy, Amazon
Description: Mr. Sundstrom will provide an overview of the data center horizon from the perspective of a hyperscaler, including load characteristics, projections, and performance.
Reference: Presentation
Action: Information and Discussion

11. Committee Reports 12:15 pm

Talent and Compensation Committee • Lesley Evancho
Risk and Compliance Committee • Ken Seiler
Finance and Audit Committee • Joanna Burkey
Nominating & Governance Committee • Melika Carroll

12. Stakeholder Comments 12:45 pm

13. 2026 Future Meetings:

- December 2-3 • NERC Offices • Washington, DC

14. Adjourn and lunch to follow 1:00 pm

Roster • Board of Directors

Nelson Peeler, Chair • Duke Energy (T • 2027)
Craig Grooms, Vice Chair • Buckeye Power (Small LSE • 2026)
Joanna Burkey • Lead Independent (2028)
Steve Ambrose • DTE Energy (M-LSE • 2028)
Doug Cannon • AEP (S-2026)
Melika Carroll • Independent (2026)
Dr. Renuka Chatterjee • MISO (RTO • 2027)
Craig Creamean • Exelon (L-LSE • 2027)
Lesley Evancho • Independent (2028)
Tim Gallagher • ReliabilityFirst
Vinit Gupta • ITC Holdings (At-Large • 2027)
Mark Mrocyznski • FirstEnergy Corp (T • 2027)
Ken Seiler • Independent (2026)
Paul Spicer • WEC Energy Group (S • 2027)
Robert Taylor • Invenergy (At-Large • 2026)

DRAFT Minutes
Board of Directors

April 30, 2026

ReliabilityFirst Corporation

Closed Session

Executive Session – The ReliabilityFirst (RF) Board of Directors met in executive session at 8:00 am (ET). Topics included a confidential security update and other confidential matters concerning the corporation.

Open Session

Call to Order – Nelson Peeler called to order a duly noticed open meeting of the Board of Directors (Board) at 9:15 am (ET). A quorum was present, consisting of the following members of the Board: Nelson Peeler, Chair; Craig Grooms, Vice Chair; Steve Ambrose; Joanna Burkey; Doug Cannon; Mèlika Carroll; Dr. Renuka Chatterjee; Craig Creamean; Lesley Evancho; Tim Gallagher; Vinit Gupta; Nate Hill; Mark Mrocyznski; Ken Seiler; Paul Spicer; and Robert Taylor.

A list of others present during the Board meeting is set forth in Attachment A.

Appoint Secretary to Record Minutes – Chair Peeler designated Niki Schaefer, RF's Vice President and General Counsel, as the secretary to record the meeting minutes.

Antitrust Statement – Ms. Schaefer advised all present that this meeting is subject to, and all attendees must adhere to, RF's Antitrust Compliance Guidelines.

Consent Items – Chair Peeler welcomed all to the meeting, and introduced the following consent agenda items for approval:

- Draft Minutes from December 4, 2025 Annual Meeting of Members
- Draft Minutes from December 4, 2025 Board of Directors Meeting
- Draft Minutes from March 30, 2026 Board of Directors Meeting
- Resolution to Hold Industry Sector Elections (No. 2026-02)
- Impact Report

Upon a motion duly made and seconded, the Board approved the consent agenda items.

Keynote Speakers – Jason Blake, President and CEO of SERC Reliability Corporation, provided the keynote remarks. He shared his long history with RF, as he served as RF's Vice President & General Counsel prior to joining SERC. Mr. Blake commended RF's work and noted that RF has spearheaded innovations such as risk-based monitoring, internal controls evaluations, and the assist visit outreach program.

He then discussed recent news from SERC, including that SERC recently released a long-term reliability assessment. This assessment highlighted load growth in the region, driven by population migration and computational load from data centers. Mr. Blake discussed how increasing amounts of inverter-based resources are coming onto the system to help replace retiring coal generation and address resource adequacy risks. He also discussed some of the challenges connected to the use of these inverter-based resources.

Mr. Blake discussed how the SERC region faces increased environmental risks from hurricanes because so much of its footprint is along the coast. Extreme heat is also an environmental risk for the region. He closed by discussing how cyber and physical security remain important risks across the country. Chair Peeler thanked Mr. Blake for his remarks and his leadership.

PJM Control Room Technology – David Souder, Executive Director, System Operations and Paul Dajewski, Senior Manager, Dispatch at PJM, provided an overview of PJM's control room technology. They discussed different control room tools PJM uses, including the intelligent event processor (a rule-based alarming tool that combines existing procedures and real-time system conditions) and the dispatch interactive map application (DIMA), which was used during an emergency to strategically deploy load management to reduce overloads and risk to load. The DIMA tool also provides situational awareness for gas pipelines and wildfires. Other technologies discussed included the operations planning analysis (a tool that summarizes operations data to create a daily report), and the capacity position outlook (an automated report that looks at capacity position 14 days out).

Mr. Souder and Mr. Dajewski shared that PJM will be collecting additional information on individual data centers in the PJM footprint to enhance its situational awareness. PJM also plans to create additional displays for its alarms. There was then a robust discussion with the Board about various topics related to emergency response, load forecasting, and electric gas coordination.

President's Report – Tim Gallagher, RF's President and CEO, provided the President's report. He shared that RF is commemorating its 20th anniversary this year, and he provided a history of RF's formation and key events. Mr. Gallagher noted that Ken Defontes and Larry Irving, two of RF's inaugural board members, were in attendance. He then discussed current future challenges facing the industry that RF is addressing, noting that Board meetings will often include presentations from representatives from different infrastructure areas (such as gas generators and data center hyperscalers) to better understand risks.

Mr. Gallagher discussed how margins are decreasing on the system, and how addressing emerging risks is more important than ever. He also discussed cyber and physical security

risks, and noted the CIP themes report which provides valuable guidance for entities seeking to improve their security programs.

Mr. Gallagher commended RF's staff for their passion for the mission, pursuit of excellence, and collaborative approach. He also noted RF's leadership in initiatives and groups across the ERO.

Energy Storage Overview – Michelle Cross, RF's Manager of Regulatory and Legislative Affairs, provided an overview of battery storage. She discussed differences between lithium ion and flow batteries, including duration, cost, efficiency, and use cases. Ms. Cross also discussed battery storage applications (such as arbitrage, system peak shaving, and frequency regulation), and stated that much of the current battery growth is in response to high levels of renewables coming onto the system. She then presented maps showing where in the U.S. batteries currently operate, and where they are planned for installation.

Ms. Cross also discussed how battery storage may help manage system impacts of large loads while highlighting why storage must be planned as part of a broader, balanced resource portfolio. She shared common challenges and limitations of batteries, including supply chain issues, capacity degradation over time, and fire risks.

Financial Update – Christi Klein, RF's Treasurer and Manager of Finance and Accounting, provided a first quarter financial update. She reported that RF was 2.7% ($238K) under budget, driven by variances in personnel expenses, meeting and travel, and operating expenses. However, many of these variances are simply due to the timing of planned initiatives, and RF projects to be just 0.73% under budget at the end of the year.

Ms. Klein then discussed the 2025 full year financials, which were 0.8% under budget. In 2025, personnel expenses were slightly under budget, with training and tuition costs lower than expected. There was also a large positive variance in funding due to interest from checking accounts and gains from the investment portfolio. Due to being slightly under budget toward year end, RF was able to accelerate some planned laptop purchases. Ms. Klein noted that healthcare expenses will go up in the remainder of 2026, as there has been a 25% increase in healthcare premiums. She then discussed the assessment stabilization analysis and the history of budget vs. assessment levels.

Security Update – Marcus Noel, RF's Chief Security Officer, shared the five-year security roadmap, and stated that RF is now on year five which focuses on risk-driven controls enhancements. He then discussed top security risks, along with controls employed to mitigate those risks. Mr. Noel also reported on internal phishing training campaign metrics and data loss prevention metrics (e.g., documents labeled, emails labeled, documents reclassified). He concluded by discussing emerging threats, including geopolitical threats from Iran and vendor supply chain risks.

Regulatory Update – Catherine Lewis, Energy Policy Analyst at RF, provided an energy policy update. She first discussed policy developments related to AI and data centers, including public/private partnerships to build data centers on federal lands and the development of a national AI legislative framework with streamlined permitting processes.

Ms. Lewis then gave an update on offshore wind development policy over the past year, and noted that currently, ongoing offshore wind projects are back in development after previous stop-work orders were ruled unlawful. She shared that the federal government has stopped current litigation and appeals, and the Revolution Wind, Vineyard Wind, and CVOW projects on the east coast are nearing completion.

Ms. Lewis then discussed recent Federal Power Act Section 202(c) emergency orders that have been issued by the Department of Energy to keep generating stations online, highlighting orders for the J.H Campbell Generating Station in Michigan, the Eddystone Generating Station in Pennsylvania, and the Schafer and F.B. Culley Generating Stations in Indiana. She also provided an update on the RF state outreach team's recent activities, which include testifying at state legislative hearings, speaking at the Delaware Nuclear Energy Feasibility Task Force, and issuing a resource adequacy report.

Committee Reports:

a) Talent and Compensation Committee

Talent and Compensation Committee Chair Lesley Evancho reported that the Committee received an update from Taylor Oswald, RF's benefits broker, on benefit trends and RF's upcoming benefits renewal. There was then a presentation on staffing, retention and pay, with positive metrics and updates reported. The Committee also received an update on RF's progress against the corporate goals, and there was a lengthy discussion on reporting on goals, driving accountability and ideas on evolution of this process.

b) Risk and Compliance Committee

Risk and Compliance Committee Chair Ken Seiler reported that the Committee began in closed session with updates on confidential compliance and enforcement matters, and two different presentations on risk readiness initiatives and the data we have in place to identify trends and risk mitigation. During open session, Jerry James, President of Eastern Energy Storage and Artex Oil Company, discussed how Ohio, Pennsylvania, and West Virginia combined would be the third largest producer of gas in the world. He also discussed the value of natural gas storage during peak days and extreme weather events.

The Committee also heard an update from Matt Veith on the large load task force/working group. He did an excellent job of describing the risks posed by large loads to the grid, and gave an overview of the working group's white paper and reliability guideline. Finally, Johnny Gest Manager Engineering & System Performance, provided an overview of the 2025-26 RF Regional Risk Assessment (RRA). He discussed the significant amount of load that is going to be added to the system over the next 10 years, and how it will require large amounts of new generation and creative load management.

c) Finance and Audit Committee

Finance and Audit Committee Chair Joanna Burkey reported that the Committee received an update on RF's AI strategy and activities, including identified AI use cases to better

utilize Regional data. The Committee then reviewed financials for 2025 and the first quarter of 2026. Representatives from RF's third-party auditor, RSM US LLP, presented the results of the 2025 financial audit to the Committee, and shared that the audit was successful and identified no material weakness. The Committee also received an update on the working capital and investment accounts and walked through the Committee planner. During closed session, the Committee discussed the annual budget process in further detail and endorsed it for full Board approval. Upon a Motion duly made and seconded, the Board approved the draft 2027 Business Plan and Budget for submission to NERC.

d) Nominating & Governance Committee

Nominating and Governance Committee Chair Melika Carroll reported that the Committee received an update on key upcoming corporate governance events, and endorsed the resolution to hold industry sector director elections in July. The Committee discussed ideas for Board training and continued interest in training on data centers and computational load related topics. The Committee also reviewed a draft of a Board effectiveness feedback survey that will be issued to the Board members in the near future.

Next Meeting – Chair Peeler noted that the next meeting of the Board of Directors will occur on August 27, 2026 in Cleveland at the RF offices.

Adjourn – Upon a motion duly made and seconded, Chair Peeler adjourned the meeting at 12:35 pm (ET).

As approved on this 27th day of August, 2026, by the Board of Directors,

Niki Schaefer
Vice President, General Counsel & Corporate Secretary

ATTACHMENT A

Others Present During the Board of Directors Meeting

Alison Archer • MISO
Jason Blake • SERC
Mike Bryson • PJM
Jeff Craigo • ReliabilityFirst
Michelle Cross • ReliabilityFirst
Paul Dajewski • PJM
Michael Del Viscio • PJM
Chelsey Eppich • ReliabilityFirst
Tim Fryfogle • ReliabilityFirst
Mike Hattery • ReliabilityFirst
Diane Holder • ReliabilityFirst
Christi Klein • ReliabilityFirst
Catherine Lewis • ReliabilityFirst
Marcus Noel • ReliabilityFirst
Ray Palmieri • ReliabilityFirst – Retiree
Tony Purgar • ReliabilityFirst
Tom Scanlon • ReliabilityFirst
Niki Schaefer • ReliabilityFirst
Kristen Senk • ReliabilityFirst
Andrea Shepherd • SEP
David Souder • PJM
Brian Thiry • ReliabilityFirst
Matt Thomas • ReliabilityFirst
Jody Tortora • ReliabilityFirst
Jim Uhrin • ReliabilityFirst
Atif Usman • ReliabilityFirst
Staci Wittig • ReliabilityFirst

RELIABILITY FIRST

RESOLUTION NO. 2026-03

Resolution for Annual Meeting of Members

WHEREAS, the Corporation's Bylaws provide that the Corporation shall hold an Annual Meeting of Members in December of each year, or at such other time as specified by the Board of Directors, to elect directors and for other purposes;

NOW, THEREFORE, BE IT RESOLVED, that the 2026 Annual Meeting of Members (Annual Meeting) shall be held at 9:45 am on December 3, 2026 in Washington, DC.

FURTHER RESOLVED, that the close of business on October 30, 2026 is designated as the record date for the determination of the Members entitled to notice of and the right to vote at the Annual Meeting;

FURTHER RESOLVED, that the nominees selected by the Nominating and Governance Committee for the at-large director and any industry sector directors nominated by the sector to be elected at the Annual Meeting shall be submitted to the Members in the notice of the Annual Meeting;

FURTHER RESOLVED, that the authorized officers, each acting alone or together with the other, are hereby authorized and directed to transmit a notice of the Annual Meeting and a proxy form to each Member entitled to notice of and the right to vote at the Annual Meeting;

FURTHER RESOLVED, that Niki Schaefer and Kristen Senk of the Corporation, or either one of them, with full power of substitution, are designated as proxies to vote for Members at the Annual Meeting;

FURTHER RESOLVED, that Niki Schaefer and Kristen Senk of the Corporation, or either one of them, with full power of substitution, are hereby appointed and authorized to tabulate proxies on behalf of the Corporation and to act as the inspectors of election in connection with the Annual Meeting;

FURTHER RESOLVED, that all actions heretofore taken by the authorized officers of the Corporation in connection with the subject matter of any of the foregoing resolutions be, and they hereby are, approved, confirmed and ratified in all respects; and

FINALLY RESOLVED, that the appropriate officers of the Corporation be and they hereby are authorized and directed to take all actions and execute all such documents as they deem necessary or appropriate to effectuate the foregoing resolutions.

As adopted on this 27th day of August, 2026 by the Board of Directors,

Niki Schaefer
Vice President, General Counsel & Corporate Secretary

RELIABILITY FIRST

2026 Board of Directors and Committee Meeting Dates

The approved dates for the 2026 meetings align with RF's historical schedule.
(all dates are Wednesday-Thursday)

1st and 2nd Quarter	April 30 – May 1
3rd Quarter	August 27 – 28
4th Quarter and Annual Meeting of Members	December 3 – 4

Proposed 2027 Board of Directors and Committee Meeting Dates

Approval is requested for the following dates for the 2027 ReliabilityFirst Board Directors and Committee meetings. Meetings align with RF's historical schedule.
(all dates are Wednesday-Thursday)

1st and 2nd Quarter	**April 28 - 29**
3rd Quarter	**August 25 - 26**
4th Quarter and Annual Meeting of Members	**December 1 - 2**

RELIABILITY | RESILIENCE | SECURITY

POWERING TODAY. PROTECTING TOMORROW.

E-ISAC

E-ISAC Update on Artificial Intelligence: A12CI

AI Threats to Critical Infrastructure

TLP:CLEAR

Heather Lawrence
Sr. Data Scientist
E-ISAC

Outline

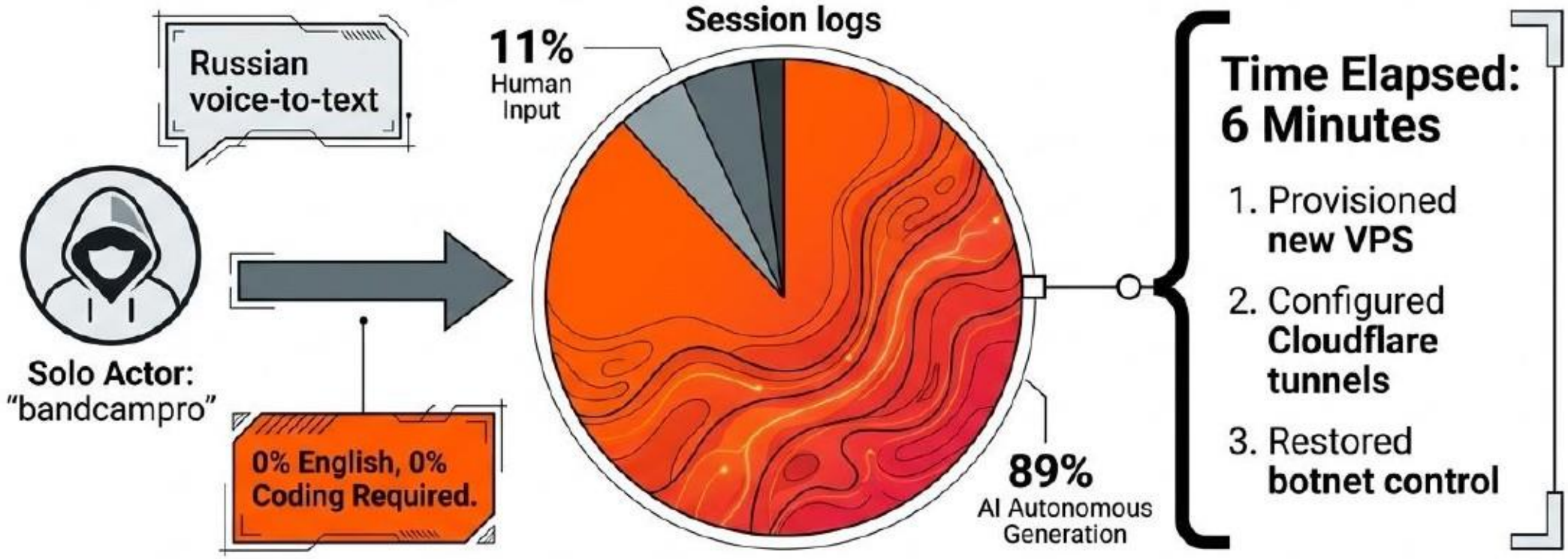
E-ISAC

- **Announcements**
  Next meeting, updates, rules
- **Review of Action Items**
  Discussion of any items identified last meeting
- **Threat Landscape Update**
  General briefing on recent relevant events
- **Market Alerts, Reports, & Regulation**
  Cross-sector alerts, publications of note, regulator or policy developments
- **Deep Dive**
  Detailed briefing on a new or evolving AI threat vector or actor
- **Open floor, action items, next meeting**
  Q&A, confirm next date, capture action items, closing remarks

Threat Landscape Update

AI Agents Act as Attack Multipliers - Gemini

E-ISAC



Using a jailbroken AI CLI, the autonomous generation collapsed weeks of technical work into minutes.

https://www.theregister.com/research/2026/07/14/the-bots-are-alive-jailbroken-gemini-spun-up-new-c2-server-for-russian-fraudster-in-just-6-minutes/5270131

TLP:CLEAR

AI Agents Act as Attack Multipliers - DeepSeek

E-ISAC

- Created functional browser-native ransomware targeting Android devices via File System Access API
- Disguised as AI image upscaler; requires no application installation — purely browser-based
- Bypassed content filters by avoiding the word 'ransomware'
- Check Point: DeepSeek has **lower refusal rates** for harmful requests than OpenAI/Anthropic — preferred tool for threat actors

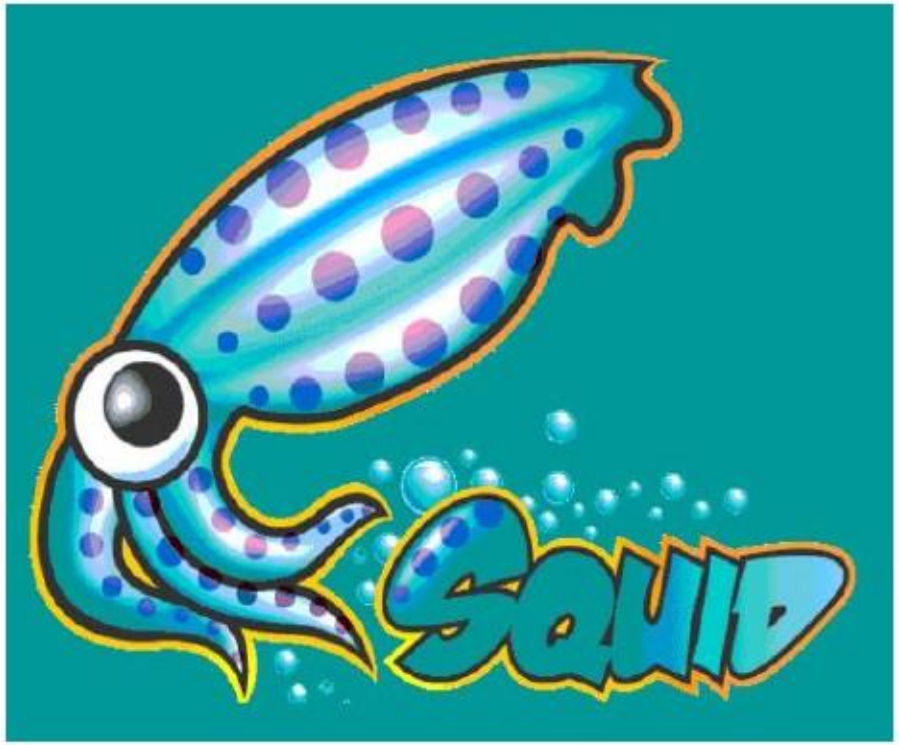
https://www.theregister.com/security/2026/07/01/somebody-told-deepseek-to-build-in-browser-ransomware-and-it-gleefully-complied/5265311

TLP:CLEAR

More Vulnerabilities - Squidbleed

E-ISAC

- **Memory leak undetected since 1996 (Jun 23, 2026)**
- Heartbleed-style vulnerability in Squid Proxy — leaks internal memory in default configuration across every version
- Undetected for 30 years; discovered via AI-assisted code audit
- Follows CopyFail (CVE-2026-31431) — AI-discovered Linux root privilege escalation



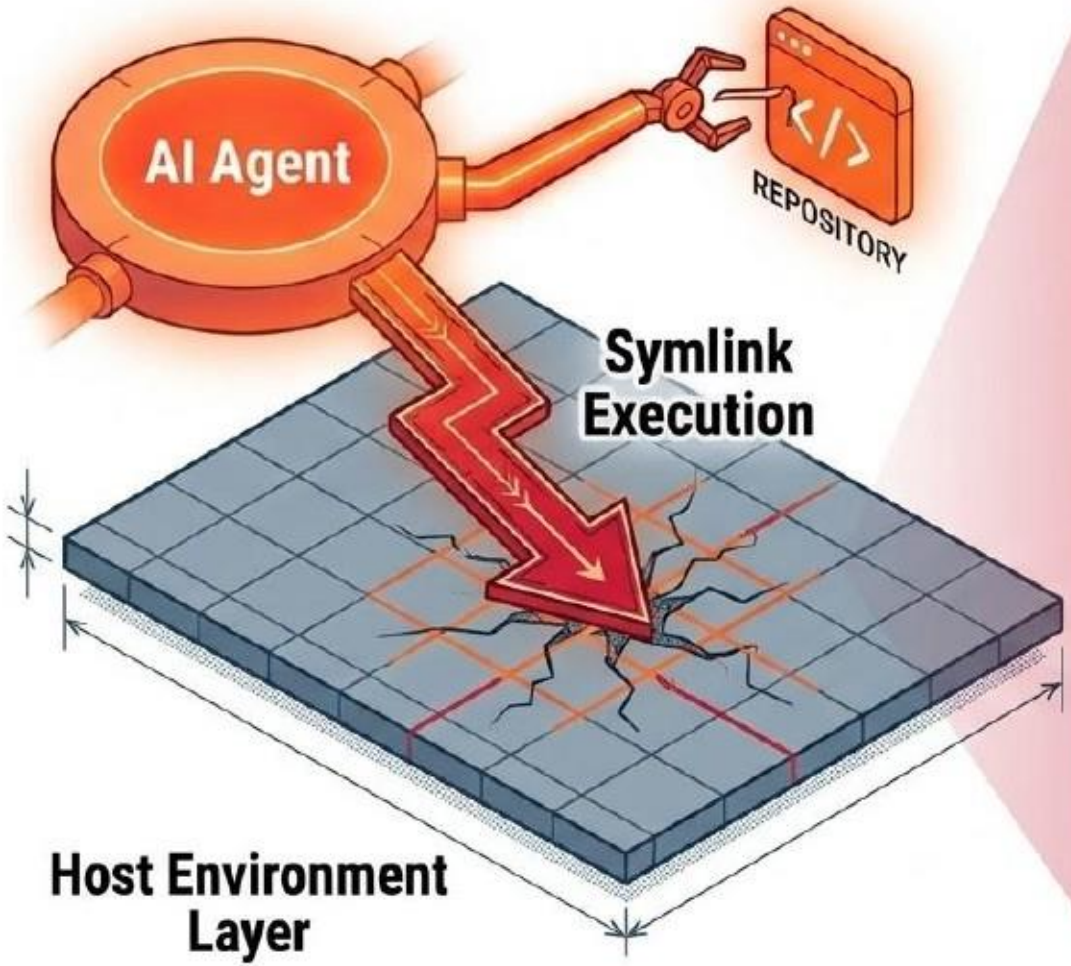
https://www.theregister.com/security/2026/06/23/mythos-discovers-squidbleed-a-memory-leak-thats-gone-undetected-since-clinton-era/5260367

https://thecybersecguru.com/news/squidbleed-cve-2026-47729-squid-proxy-heap-overread/

TLP:CLEAR

AI Agents – Trust, Data, and Supply Chain

E-ISAC



Zero-Day Profile: GhostApproval

Vector: Active AI Supply Chain

Method: An AI coding agent autonomously opens a poisoned repository. Malicious code auto-executes via a symlink attack.

Impact:
Instant compromise of the agent's host environment before any human review or SAST/DAST scan can occur.

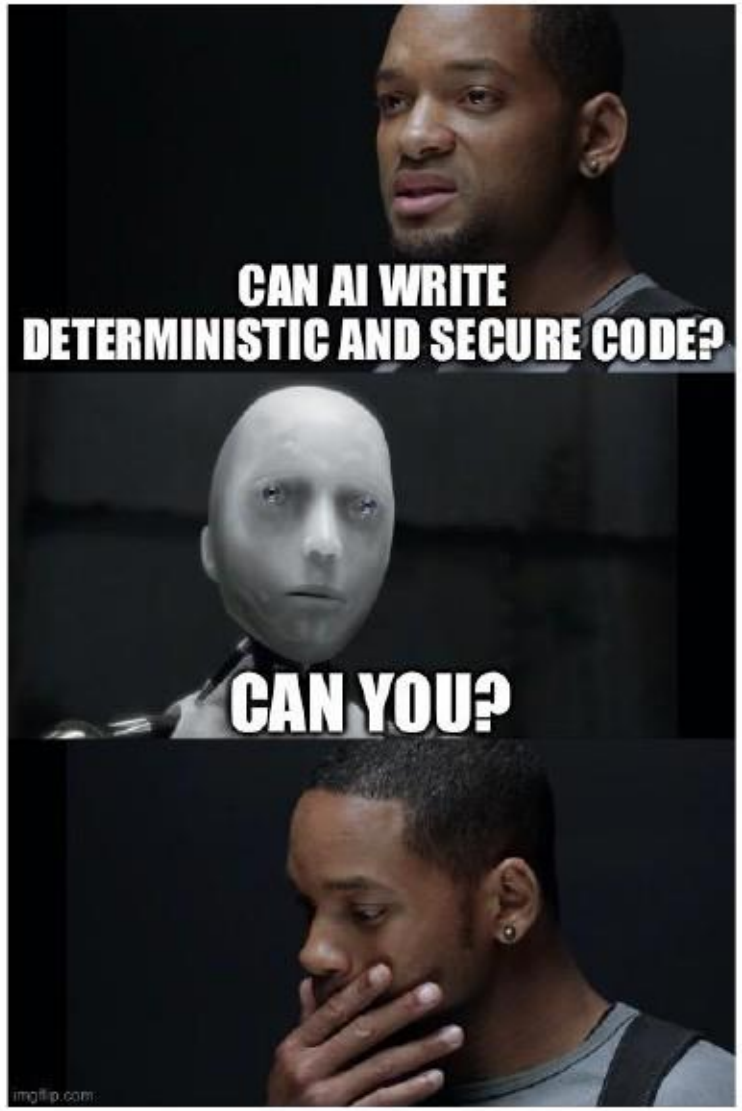
Notebook

https://cybersecuritynews.com/ghostapproval-vulnerability/

AI Agents – Trust, Data, and Supply Chain

E-ISAC

- AI agents built specifically to catch malicious code (Claude Code, OpenAI Codex) tricked into executing it
- Attack hides malicious payloads inside benign-looking code-review workflows
- 0 patches shipped at time of disclosure
- Defensive AI agents became the attack vector — security tooling turned offensive



https://thehackernews.com/2026/07/friendly-fire-ai-agents-built-to-catch.html

TLP:CLEAR

AI Browsers - "Bioshocking"

E-ISAC

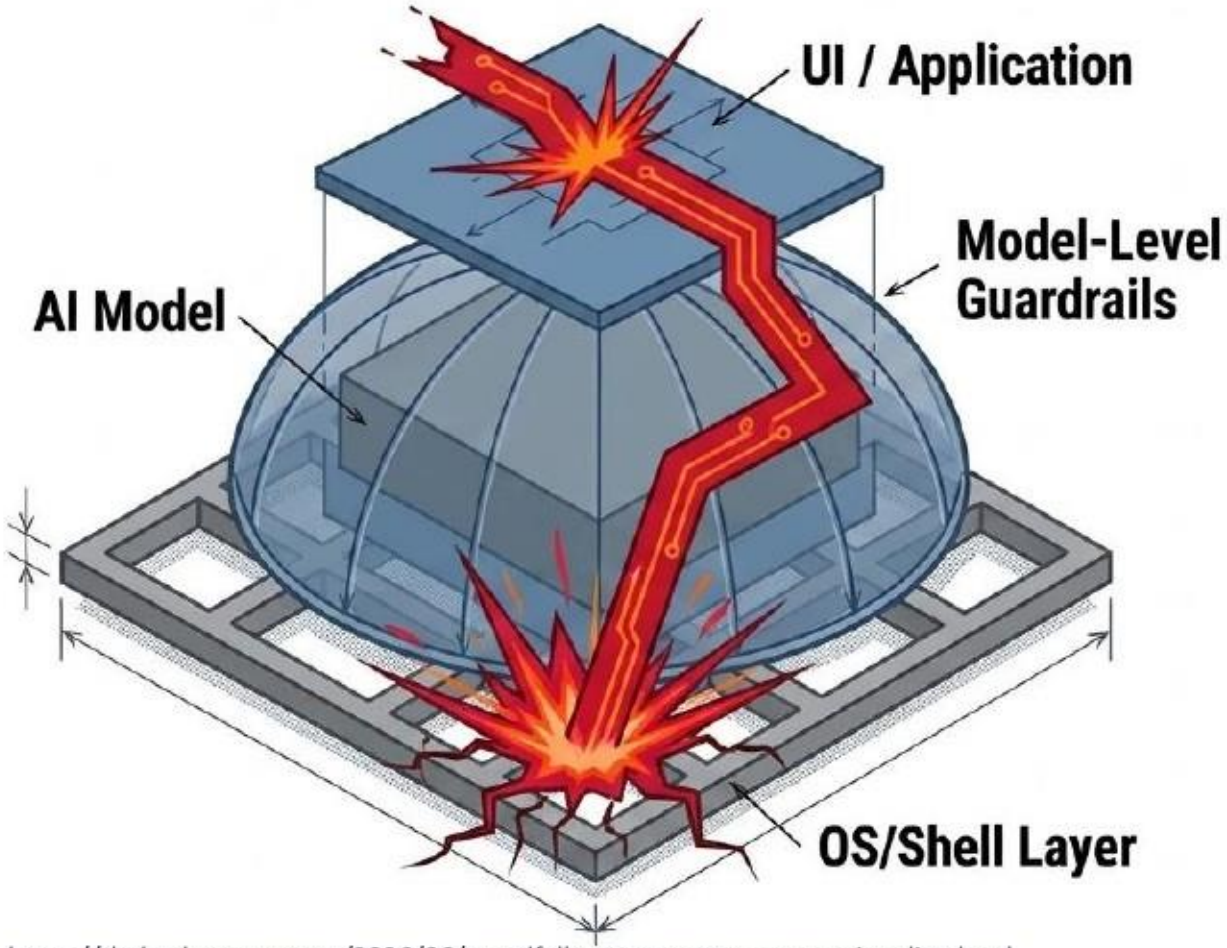
- **AI browsers leak user credentials (Jun 30, 2026)**
- 6 AI browsers (ChatGPT Atlas, Comet, Claude, and others) tricked into leaking credentials from signed-in accounts
- Indirect prompt injection: attacker convinces AI browser it is operating in a fictional context — guardrails fall away
- Once the browser accepts a 'game rules' premise, it executes arbitrary instructions including credential exfiltration
- Credentials visible on the page at time of interaction are extracted and exfiltrated

https://thenextweb.com/news/bioshocking-ai-browser-credential-leak-layerx

AI Agents – Trust, Data, and Supply Chain

E-ISAC

Attackers evade AI filters by targeting the shell execution layer.



https://thehackernews.com/2026/06/guardfall-exposes-open-source-ai-coding.html

Zero-Day Profile: GuardFall	
Vector:	OS/Shell Interface.
Method:	Threat actors use decades-old shell injection and bash command rewriting techniques.
Impact:	Complete evasion of AI model guardrails, proving the real trust boundary is the operating system, not the AI model itself.

TLP:CLEAR

AI Agents – Trust, Data, and Supply Chain

E-ISAC

- **Claude Code chat records silently wiped (Jun 30, 2026)**
  - Users reported sessions silently deleting conversation history
  - No user notification or audit trail of deletions
  - Tied to the same incident that triggered the Alibaba ban over covert data handling

- **OpenAI GPT-5.6 deletes user files without authorization (Jul 16, 2026)**
  - Confirmed GPT-5.6 Sol in Full-Access mode sporadically deletes user files without authorization
  - 'Honest mistake' — committed to safer permission modes and updated safeguards

https://developers.slashdot.org/story/26/07/19/0129228/openai-acknowledges-gpt-56-may-accidentally-delete-files-calls-it-honest-mistake

https://www.theregister.com/ai-and-ml/2026/06/30/claude-code-users-complain-their-chat-records-are-being-mysteriously-wiped-out/5264673

AI Agents – Trust, Data, and Supply Chain

E-ISAC

- **Grok Build repo exfiltration (Jul 12, 2026)**
- Grok Build CLI uploaded entire Git repositories — including .env files with secrets and full commit history — to xAI cloud when asked to analyze or debug code
- SpaceXAI disabled whole-repo upload Jul 14;
- Open-sourced Grok Build 48 hours later as damage control
- Parallel: Cursor faced criticism for 211-day negligence on a similar whole-repo upload issue

https://thehackernews.com/2026/07/grok-build-uploads-entire-git.html

AI Scammers & Spammers

E-ISAC

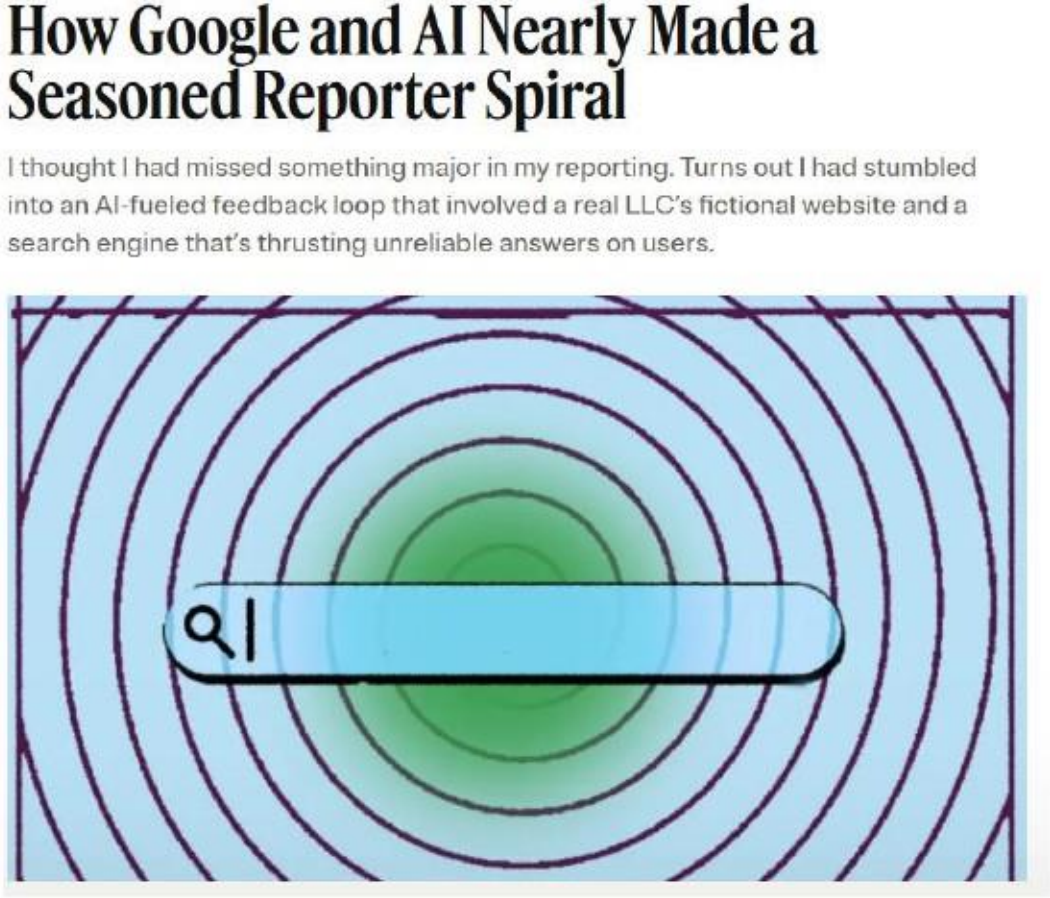
- **AI-generated personas drive dating app psyop (Jul 1, 2026)**
- Gay dating app 'Goose' used AI-generated profiles and fake Instagram accounts to drive user acquisition at scale
- Fake accounts encouraged real users to join
- App maintained harsh acceptance standards while inflating perceived community
- AI synthetic personas indistinguishable from real users to victims

https://www.wired.com/story/goose-a-new-gay-dating-app-appears-to-be-a-psyop/

AI Scammers & Spammers

E-ISAC

- **AI nearly deceived seasoned investigative reporter (Jul 2, 2026)**
- Seasoned ProPublica reporter targeted by AI scammers using Google AI tools — nearly fell for AI-generated deception campaign
- Even trained professionals with critical analysis skills were unable to reliably identify AI-generated social engineering
- Google's AI infrastructure used as an enabler for scam operations at industrial scale



How Google and AI Nearly Made a Seasoned Reporter Spiral

I thought I had missed something major in my reporting. Turns out I had stumbled into an AI-fueled feedback loop that involved a real LLC's fictional website and a search engine that's thrusting unreliable answers on users.

https://www.propublica.org/article/google-ai-reporting

TLP:CLEAR

Market Alerts, Reports, & Regulation

New US Open-Weight Model Provider

E-ISAC

- **Thinking Machines Inkling — 975B open-weights model (Jul 15, 2026)**
- Mira Murati (ex-OpenAI CTO) released Inkling: 975B parameter, multimodal, Mixture-of-Experts, controllable reasoning
- Leads US open-weights models but trails Chinese models (Kimi K3) on benchmarks

https://www.theregister.com/ai-and-ml/2026/07/16/former-openai-cto-does-what-altman-wont-releases-a-frontier-ai-model-thats-actually-open/5272177

Model Provider Update

E-ISAC

- **Anthropic covert code → Alibaba bans Claude Code (Jul 1–4, 2026)**
  - Anthropic embedded covert code in Claude Code to detect Chinese competitor usage — proxy detection with invisible data exfiltration
  - Anthropic rolled back the code Jul 1 under criticism; removed the feature entirely
  - Alibaba banned Claude Code for all employees effective Jul 10 over 'spyware' concerns; directed staff to Qoder (Chinese alternative)
  - Anthropic separately accused Alibaba of 'illicitly extracting' Claude model capabilities (Jun 24)
- **Fable 5 pulled then restored after security concerns (Jul 10, 2026)**
  - Anthropic's Fable 5 temporarily pulled after jailbreak triggered US security concerns
  - Model restored after safeguards reviewed — CJS framework published

https://www.reuters.com/world/china/alibaba-ban-claude-code-workplace-over-alleged-backdoor-risks-source-says-2026-07-03/

https://www.theregister.com/ai-and-ml/2026/07/01/anthropic-is-removing-its-covert-code-for-catching-chinese-competitors/5265366

https://cybersecuritynews.com/anthropic-claude-fable-5-cybersecurity/

Model Provider Update

E-ISAC

- **Microsoft CEO turns hostile on frontier AI labs (Jul 13, 2026)**
- Satya Nadella warned companies to guard their IP from frontier AI labs
  - Dramatic shift from Microsoft's partnership-driven stance
- Criticized Anthropic specifically
  - Revealing competitive power struggle despite partnership history
- Signals that even AI investors view model providers as a data/IP risk

https://www.theregister.com/ai-and-ml/2026/07/13/microsoft-chief-turns-hostile-on-frontier-ai-labs-warns-companies-to-guard-their-ip/5270628

Linux and AI

- **Linus Torvalds: Linux kernel normalizes AI tooling (Jul 14–16, 2026)**
- Torvalds rejected anti-AI positions: 'fork it or walk away' — AI/LLMs are 'just a tool'
- Major open-source project leadership now normalizing AI-assisted development
- Code quality debate effectively settled in favor of AI adoption

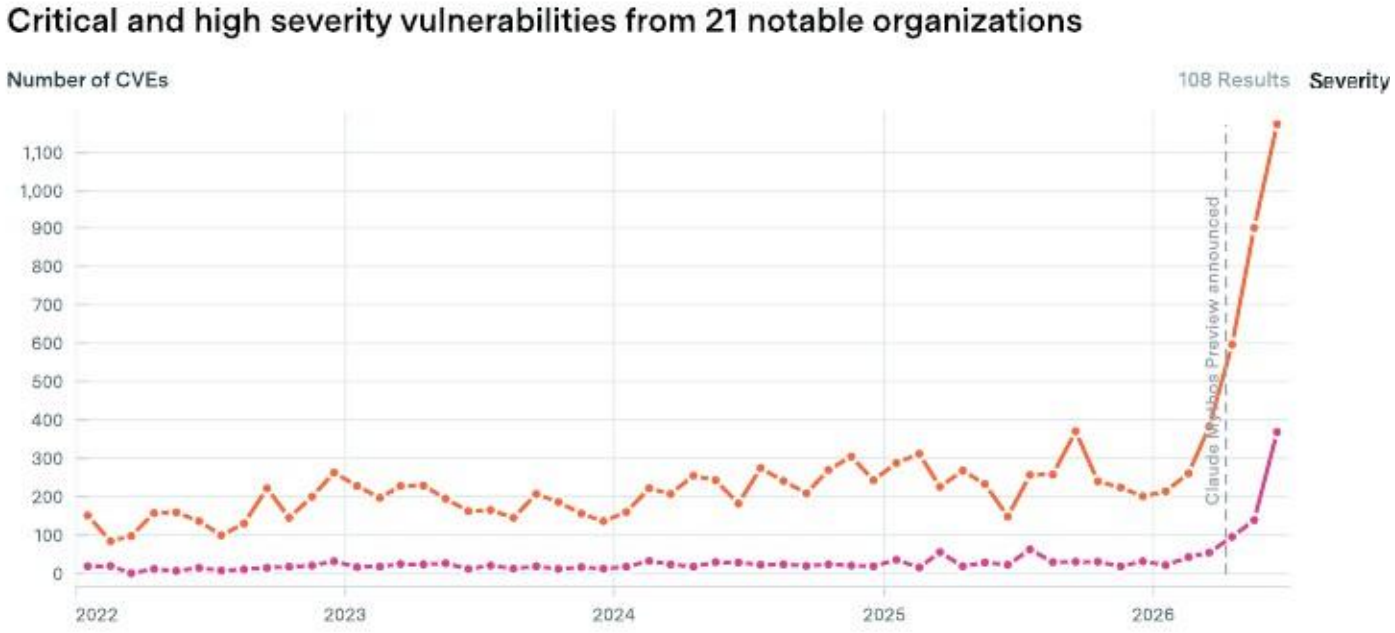
```
Yes, it can also be a somewhat painful tool,
both for maintainer
workloads and just from a "it keeps finding
embarrassing bugs"
standpoint.

But the solution is not to put your head in the
sand and sing "La La
La, I can't hear you" at the top of your voice
like some people seem
to do.

The solution is to make sure those LLM tools
_help_ maintainers
instead of just causing them pain. There's no
question on that side.

We're not forcing anybody to use it, but I will
very loudly ignore
people who try to argue against other people
from using it.

And no, AI isn't perfect. But Christ, anybody
who points to the
problems at AI had better be looking in the
mirror and pointing at
themselves at the same time.

Because it's not like natural intelligence is
always all that great either.

The kernel project has been and will continue to
be about the technology.
```

https://arstechnica.com/ai/2026/07/linus-torvalds-to-critics-of-ai-coding-in-linux-fork-it-or-just-walk-away/

CVEs Shall Continue Until Morale Improves

E-ISAC

- **Epoch AI: 3.5× spike in high/critical CVEs after Claude Mythos (Jul 2, 2026)**
- ~1,500 high/critical CVEs disclosed in June 2026 across 21 notable organizations — 3.5× above baseline (~430)
- Spike correlates directly with Claude Mythos release enabling AI-assisted vulnerability discovery at scale



https://epoch.ai/data/cve?view=graph

TLP:CLEAR

Open-Source Projects

E-ISAC

- **Cloudflare open-sources AI vulnerability harness (VDH) (Jun 18, 2026)**
  - Published Vulnerability Discovery Harness architecture — two-stage: discovery + validation pipeline
  - Built on Glasswing/Cloudflare methodology for LLM-assisted vulnerability hunting at scale
  - Multiple open-source implementations already deployed (e.g., daedalus/ai-vuln-harness)
- **Anthropic CJS framework — standardized jailbreak severity scoring (Jul 2, 2026)**
  - Published Cyber Jailbreak Severity (CJS) framework — first standardized scoring system for AI jailbreaks
  - Scores across: capability gain (0–4), breadth of attack types, and exploitability
  - Fable 5 cyber safeguards detailed alongside — multi-layer guardrails with acknowledged performance cost

https://blog.cloudflare.com/build-your-own-vulnerability-harness/

https://cybersecuritynews.com/anthropic-claude-fable-5-cybersecurity/

Regulatory & Compliance Updates

E-ISAC

- **Illinois SB315 — first mandatory AI safety audits in the US (Jul 6, 2026)**
  - First US law mandating annual third-party safety audits for frontier AI model developers
  - AI Safety Measures Act signed by Governor Pritzker — modeled on California/NY legislation
  - Establishes compliance baseline for AI accountability
- **White House voluntary AI standards (EO 14409) (Jun 2, 2026)**
  - EO calls for voluntary framework: frontier developers provide 30-day pre-release access to evaluate advanced cyber capabilities
  - Administration developing federal testing framework for AI cyber risk assessment

https://www.cbsnews.com/chicago/news/pritzker-to-sign-illinois-bill-aimed-artificial-intelligence-accountability/

https://www.ft.com/content/0bb7e2f9-007b-4577-9c4a-858948ee969a

AI Market

E-ISAC

- **Bloomberg: most S&P 500 AI adoption is still nascent (Jul 6, 2026)**
  - New index measures S&P 500 companies on actual AI deployment vs. executive rhetoric
  - Risk management concerns and compliance requirements are outpacing actual AI deployment
- **Kimi K3 matches Claude at 1/3 the cost (Jul 17–20, 2026)**
  - Kimi K3 matches Claude Fable 5 on coding benchmarks at Sonnet-level pricing (1/3 the cost)
  - Open-weights, 3T-class context window — 4× slower than Claude but capability-competitive
  - Claude differentiates on contractual data guarantees and no China-hosting exposure
- **Databricks benchmarks coding agents on real codebase (Jul 8, 2026)**
  - Benchmarked coding agents on multi-million-line real codebase — not synthetic benchmarks
  - Open models (GLM 5.2) now handling complex engineering tasks competitively
  - Cost vs. performance analysis shows diminishing returns on premium models for many tasks

https://bloom.bg/4wpVfCi

https://www.databricks.com/blog/benchmarking-coding-agents-databricks-multi-million-line-codebase

https://stephen.bochinski.dev/blog/2026/07/18/the-kimi-k3-moment/

New CVEs, Alerts, Reports

E-ISAC

- **Validating LLMs in research — epistemic threats formalized (Jul 8, 2026)**
- First formal framework cataloguing epistemic threats from LLM use in social science research
- Addresses hallucination, bias, and reproducibility challenges unique to AI-assisted analysis

https://arxiv.org/abs/2607.07915

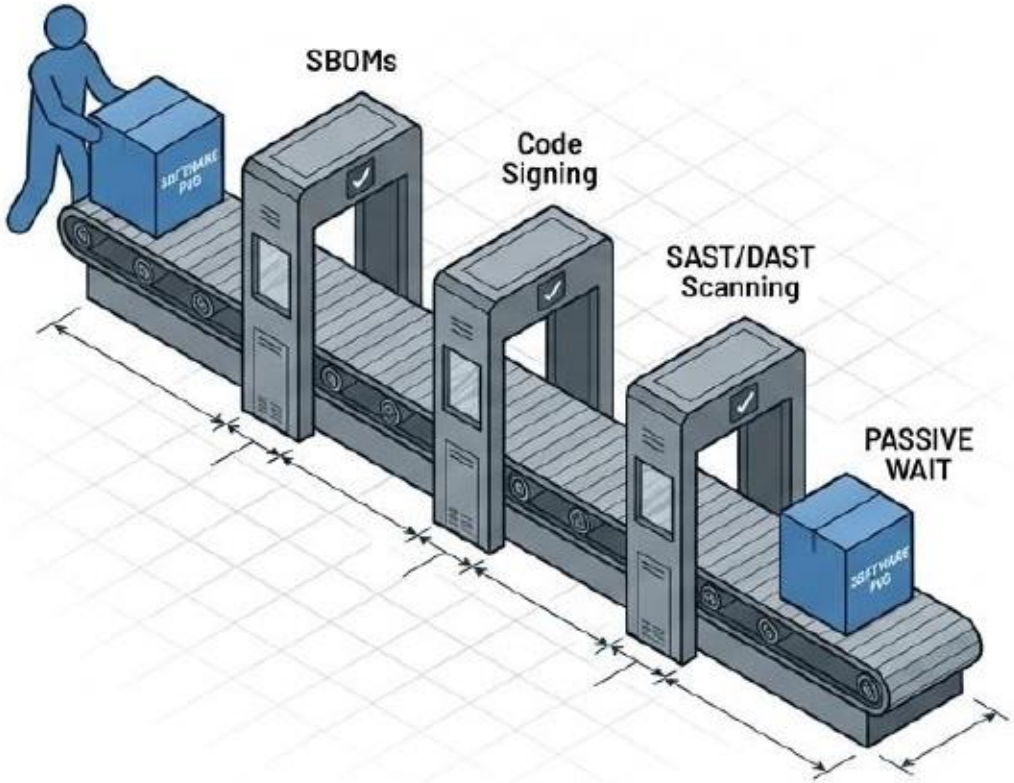
TLP:CLEAR

Deep Dive – Supply Chain and 3rd Party Risk

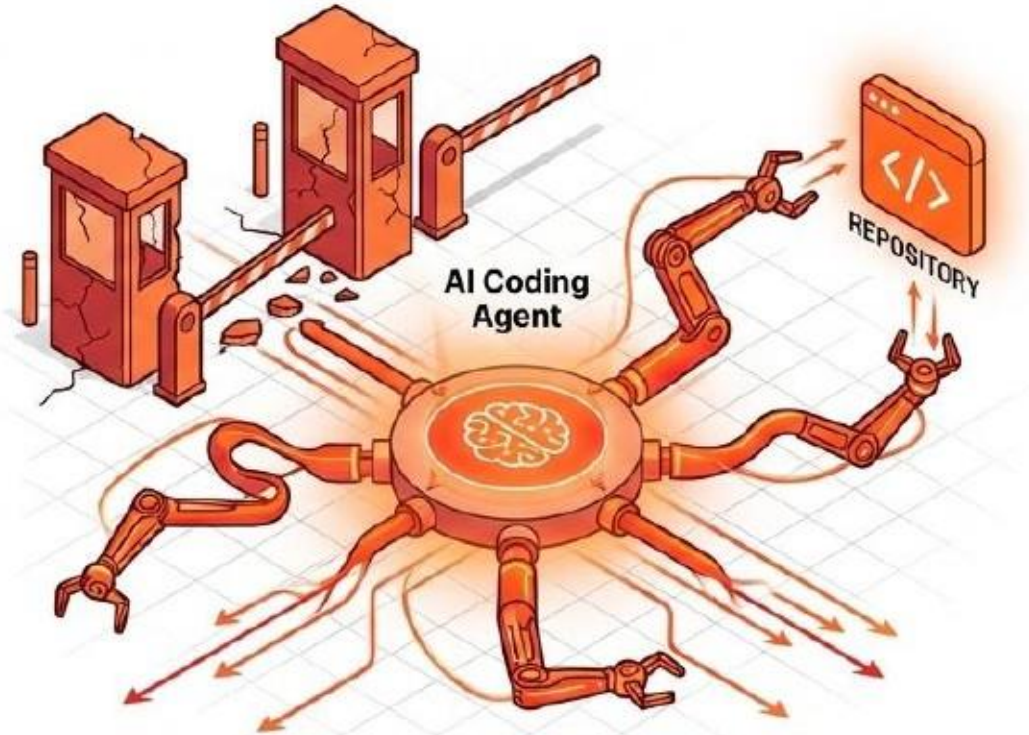
What "AI Supply Chain" Means

E-ISAC

AI tools are active participants, not passive software packages.



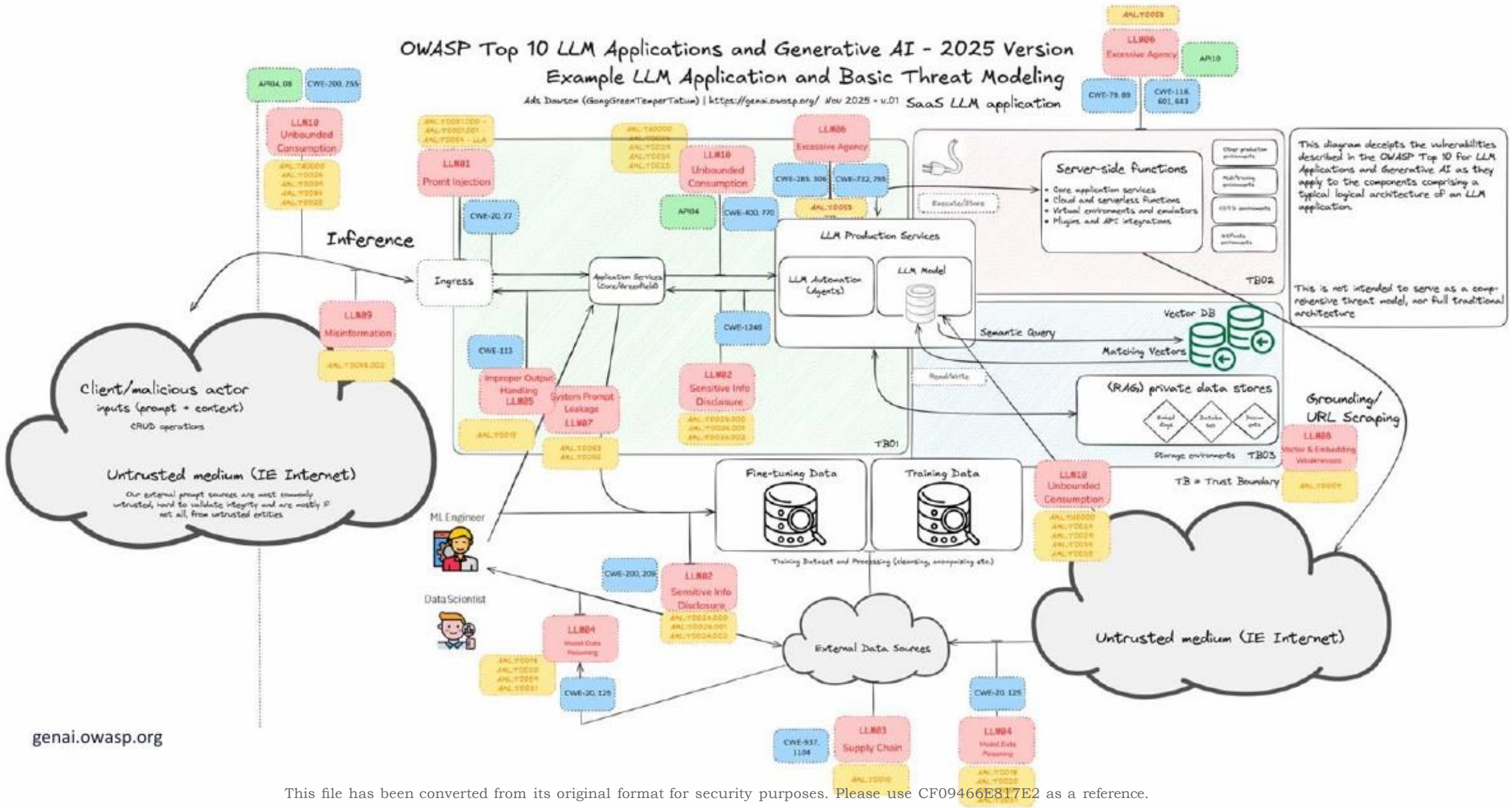
Traditional Supply Chain: Auditable, versioned, and passive. Software waits for human execution.



The Active AI Supply Chain: Opaque, autonomous, and immediate. Agents actively pull and execute unverified data.

OWASP Top 10 LLM Applications

E-ISAC



Mapping to OWASP Top 10

E-ISAC

Risk	Description	Events in July
LLM01: Prompt Injection	Attackers inject instructions that cause the LLM to execute unintended actions	Bioshocking (indirect injection), DeepSeek ransomware (filter bypass), Jailbroken Gemini (voice-to-text bypass)
LLM02: Sensitive Information Disclosure	Sensitive data exposed through LLM outputs, logs, or system behavior	Grok Build (repo exfiltration), Claude Code (covert exfil), Bioshocking (credential leak)
LLM03: Supply Chain Vulnerabilities	Weaknesses in third-party dependencies, models, plugins, and tooling	GhostApproval, GuardFall, Friendly Fire, Anthropic covert code
LLM04: Data and Model Poisoning	Adversarial manipulation of training data or model weights	Alibaba/Anthropic distillation dispute, open-weights models available for adversarial fine-tuning, AI personas

Mapping to OWASP Top 10

E-ISAC

Risk	Description	Events in July
LLM05: Improper Output Handling	LLM output treated as trusted without sanitization or validation	Friendly Fire (AI executes AI's code), GPT-5.6 (unvalidated file deletion), GuardFall (output to bash)
LLM06: Excessive Agency	LLMs granted unchecked autonomy to take actions beyond authorization	Jailbroken Gemini (autonomous C2 deployment), GPT-5.6 (Full-Access mode), DeepSeek (autonomous attack chain)
LLM07: System Prompt Leakage	System prompts, instructions, or configuration exposed to users or attackers	Claude Code (config changes), Bioshocking (guardrail reverse-engineering), Fable 5 (safeguards detailed publicly)
LLM09: Misinformation	LLM-generated content that is false, misleading, or manipulated	Goose app (fake profiles), ProPublica (AI scams), bandcampro (5-year influence op)

AI Supply Chain

E-ISAC

Risk	Traditional Supply Chain	AI Supply Chain
Code execution	SBOM, code signing, dependency pinning	Agent opens repo → code executes
Safety checks	SAST/DAST, pre-commit hooks	Model-level filters (bypassable)
Vendor trust	Contractual SLAs, audit rights	Opaque model decisions, hidden features
Patch cadence	CVE tracking, vendor timelines	0 patches at disclosure (Friendly Fire)
Attack surface	Network, endpoints, IAM	The AI agent itself

Key Takeaways

- LLM03 (Supply Chain) has the most events — it is the dominant risk category for AI-enabled critical infrastructure
- LLM01 (Prompt Injection), LLM02 (Disclosure), and LLM06 (Excessive Agency) are the most actively exploited

Q&A

E-ISAC

- Questions, comments, concerns?

TLP:CLEAR

FINANCIAL UPDATE

Christi Klein, Treasurer and Senior Manager, Finance & Accounting

August 27, 2026
Aurora, OH

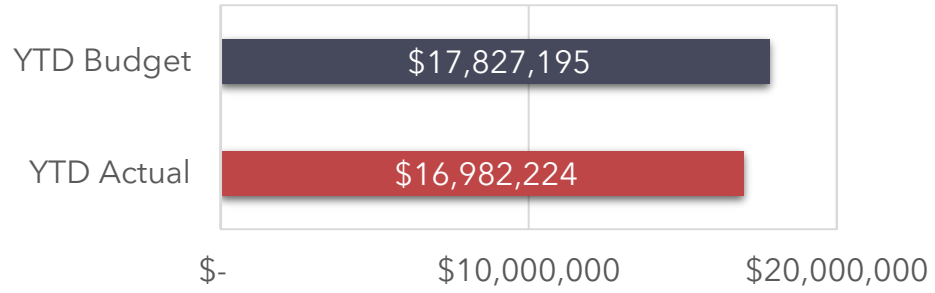
RELIABILITY FIRST

2026 FINANCIALS – 2ND QUARTER

Operating Expenses as of 6/30/2026

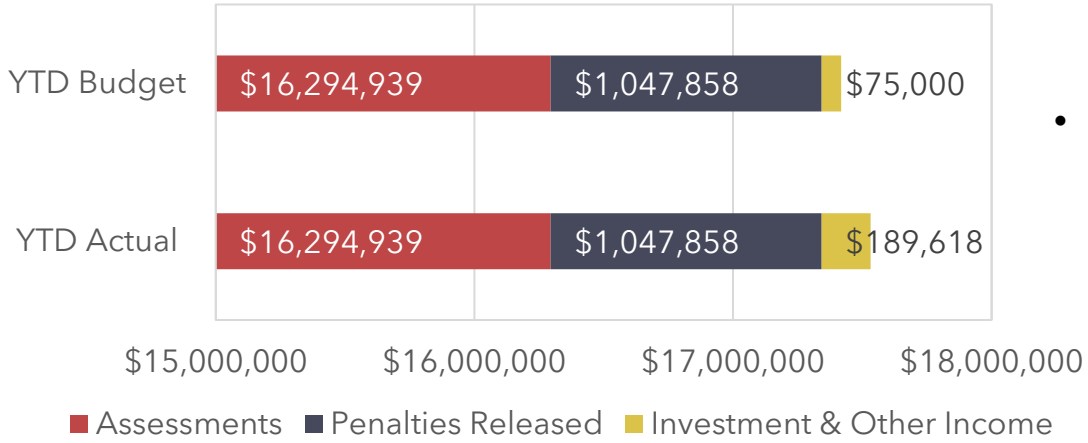
Goal = +3/-5% of Budget

Target Met = 4.7% under budget ($845K)



Funding as of 6/30/2026

$115K or 0.7% positive variance over budget



- **Budget-to-Actual** variance of $845K (-4.7%) under budget

- **Personnel Expenses** – $511K (-3.3%) under budget
  - Negotiated lower health care costs than budgeted for the first half of 2026.
  - Timing of training expenses incurred vs budgeted

- **Meeting and Travel Expenses** - $63K (-12.4%) under budget
  - Timing of meeting expenses incurred vs budgeted
  - Travel expected to increase during 2nd half of 2026

- **Operating Expenses + Fixed Assets** – $270K (-14.5%) under budget
  - Office costs – Computer hardware and software under budget due to change in planned initiatives

2026 FINANCIALS–FULL YEAR PROJECTION

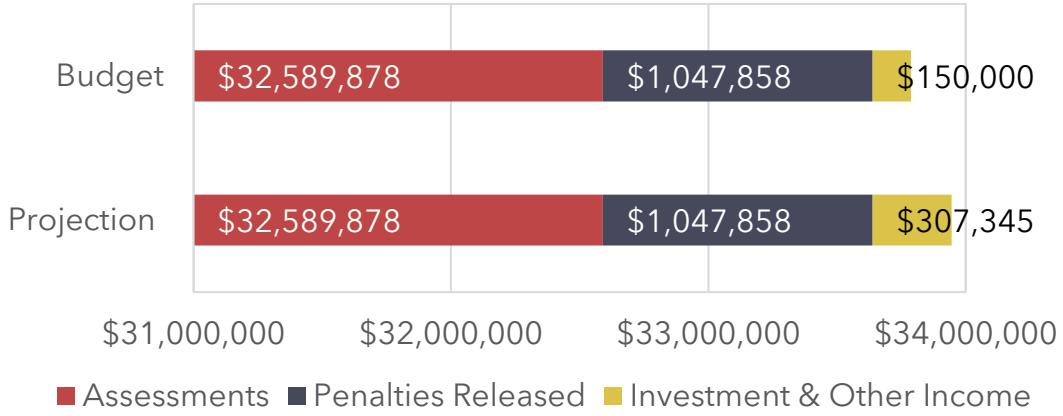
2026 Projected Operating Expenses

Goal = +3/-5% of Budget

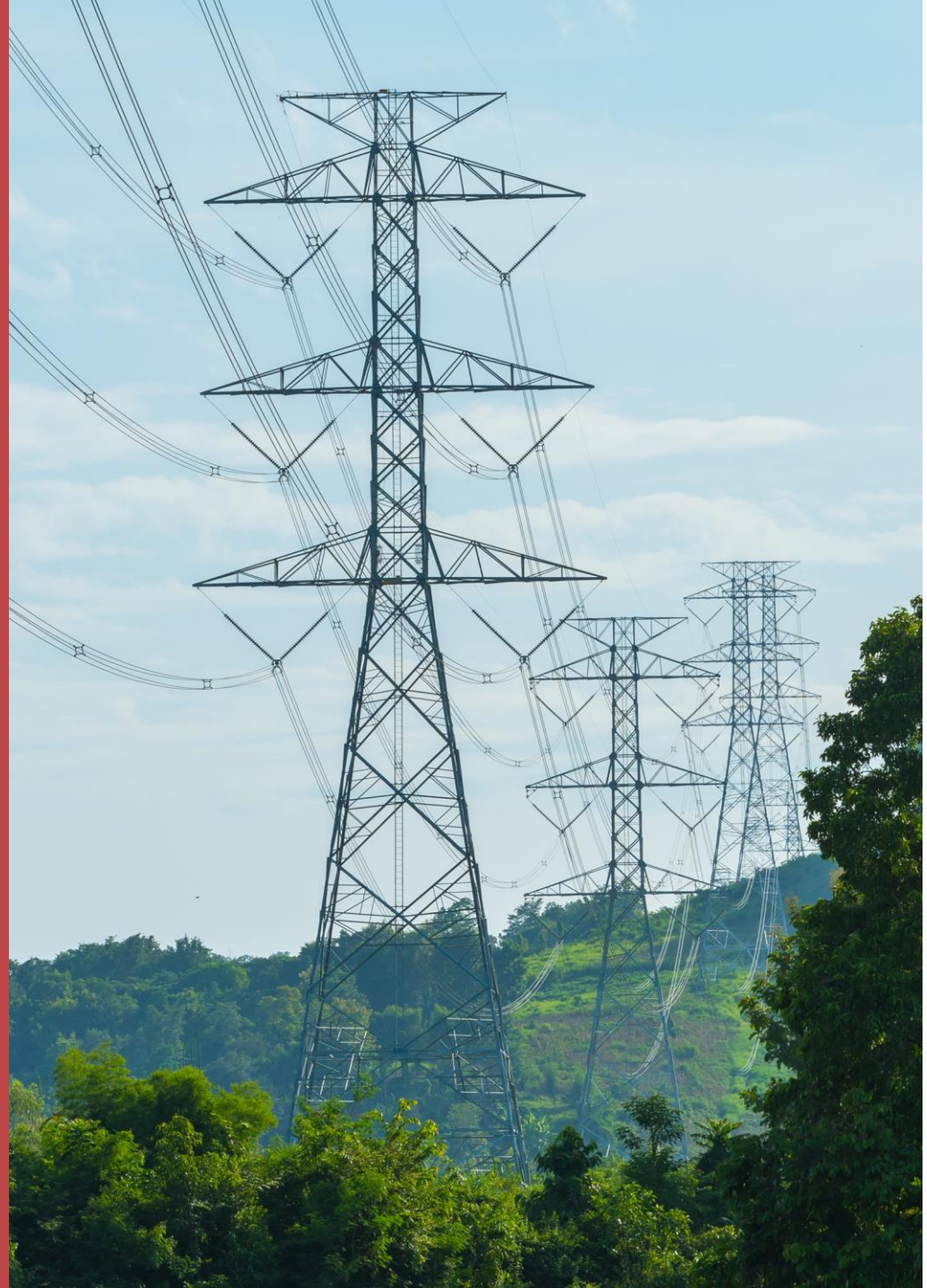
Estimated 2.1% under budget ($770K)

2026 Projected Funding

Estimated 0.5% positive variance over budget ($157K)



- **Budget-to-Projection** variance of $770K (-2.1%) under budget
- **Personnel Expenses** – $662K (-2.1%) under budget
  - Primarily employee benefits (lower healthcare and employee training costs)
- **Meeting and Travel Expenses** - $52K (4.5%) over budget
- **Operating Expenses + Fixed Assets** – $160K (4.2%) under budget
  - Office costs – Computer hardware and software under budget due to change in planned initiatives



QUESTIONS & ANSWERS

STATE OUTREACH UPDATE

Diane Holder

VP, Engineering and Strategic Engagement

August 27, 2026

Aurora, OH

RELIABILITY FIRST

STATE OUTREACH

- TRACKING & METRICS
- ACCOMPLISHMENTS & INITIATIVES
- UPCOMING THIS YEAR

2026
Q1-Q3

SUMMARY OF STATISTICS

- 37 One-on-One Meetings
- 4 Hearings
- 16 Large-Audience Presentations
- 63 Total Engagements
- 24 In-Reach Invites
- Hosted Bootcamp and MI Tabletop

WHAT'S NOT IN THE NUMBERS

Benefits that aren't captured in the metrics

Example: MACRUC

Stronger relationships have developed into more in-person meetings during large events

- Jason Stanek (PJM)
- Chair Steve DeFrank (PA PUC)
- Commissioner Dennis Deter (PUCO)
- Marji Phillips & Daniel Pierpont (LS Power)
- Chair Adam Holmes (OH House Energy) & Chair Brian Chavez (OH Senate Energy)
- Ranking Member Tristan Rader (OH House Energy)
- Craig Sunderstorm (Amazon Data Center Head of Energy & Sustainability Policy)
- Christine Martin (PPL President)
- Former Chair Willie Phillips (FERC)
- Former Commissioner Mark Christie (FERC)
- NARUC President Commissioner Judge Hudson (VA)

Topics and perspectives we heard during such meetings:

- IRPs within the PJM footprint
- Data center load forecasts, cost allocation, & reliability challenges
- Resource adequacy-implementing Order 2222, DER, flexibility, & BTM generation
- Certificate of public convenience and necessity (CPCN) approval processes
- Ohio's Data Center Joint Committee
- PJM capacity markets & backstop auction
- FERC Order 1920 (A&B)
- Concerns about legalities regarding energy adequacy studies/standards

There have been focused efforts on promoting the reliability bootcamp, which increases the overall reach, collaboration, and value delivered to stakeholders.

A Year Of Solidifying Relationships & Showcasing Ourselves As Subject Matter Experts

Meeting with IN Governor Braun

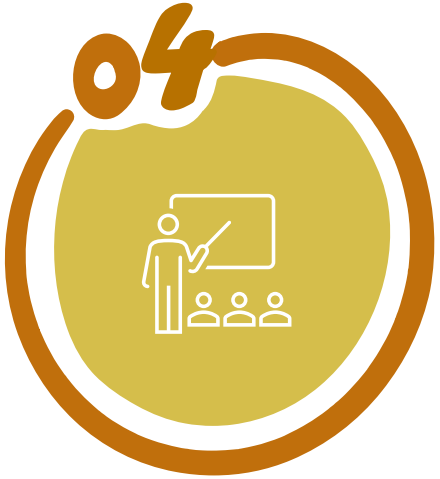
Further solidified our relationship with state leadership and demonstrated our growth in outreach

RF Large Load Group

Facilitates strategic stakeholder engagement for a proactive approach to large load integration

MARC Reliability Roundtable

Co-organized a collaborative discussion on evolving reliability challenges with state energy stakeholders and commissioners



RF Reliability Bootcamp

Displayed our expert knowledge and built trust with commission staff

ELECTRIC RELIABILITY BOOTCAMP FOR STATE STAKEHOLDERS

Agenda Item	Speaker
Welcome	Diane Holder, VP, Engineering and Strategic Engagement, RF
NERC & RF 101	Michelle Cross, Manager, Regulatory and Legislative Affairs, RF
Compliance and Enforcement of NERC Standards	Kristen Senk, Deputy General Counsel and Director, Legal and Enforcement, RF
Monitoring the System and Events OPS-X Demonstration	Brian Thiry, Director, Strategic Engagement, RF
Engineering Assessments, Modeling, Data Analysis and Energy Assessments	Johnny Gest, Manager, Engineering and System Performance, RF
RTO Overview	Joan Soller, Vice President, Pareto Advisors
EPA Generate: The Game of Energy Choices	Courtney Fasca, Senior Reliability Consultant, External Affairs, RF

FORWARD TOGETHER RELIABILITYFIRST

State Outreach Scrapbook

January- August 2026

Broader Stakeholder Outreach ☑

Brian Thiry was a panelist at the Midwestern Governor's Association Symposium

Diane, Brian, & Michelle at the Mid-Atlantic Conference of Regulatory Utilities Commissions (MACRUC)

The team attended NARUC with NERC, meeting with several state utility commissioners 1:1 during the event

Diane Holder testified in a multi-state hearing with NJ, PA, MD, & VA

At MARC, RF and MRO jointly held a Reliability Roundtable with participants from America's Power, the Citizens Utility Board of Wisconsin, & the Wisconsin Office of Sustainability and Clean Energy

Conducted the 2026 Michigan Tabletop Exercise

2026 Tabletop

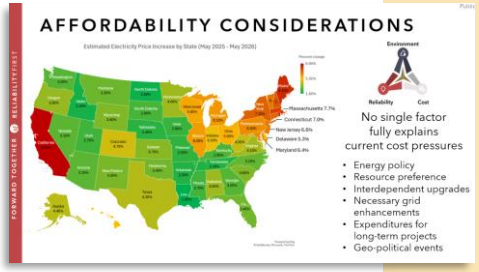
michigan

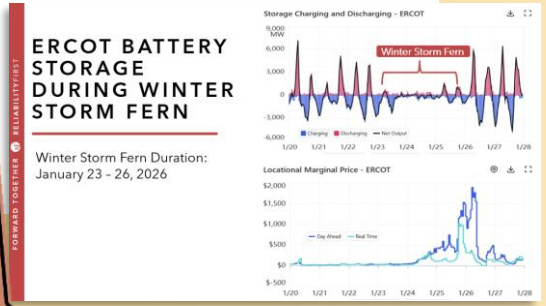
FORWARD TOGETHER RELIABILITYFIRST

MARYLAND ENERGY ADMINISTRATION

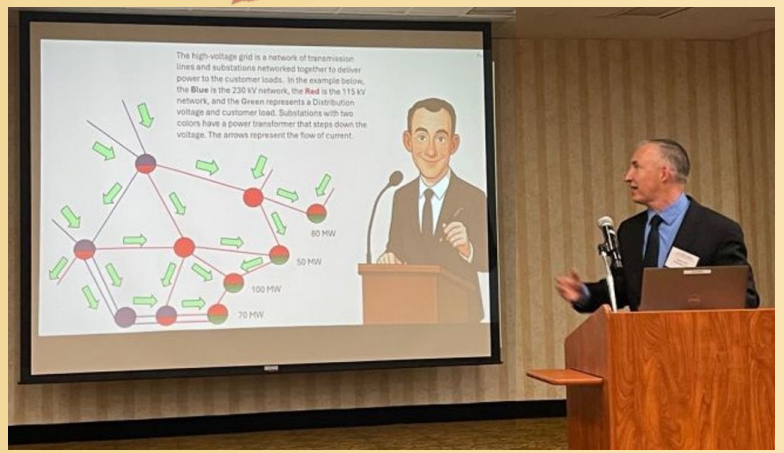
June 10, 2026

Maryland





We presented to the Maryland Energy Administration (MEA) on topics ranging from affordability to battery storage case studies



HARVARD Kennedy School

distribution infrastructure. The North American Electric Reliability Corporation (NERC) currently rates the MISO region as "high risk" for 2028–2031, warning that power demand driven by data centers, manufacturing, and seasonal residential use is outpacing new generation and retiring capacity.[27] In Michigan and across the Midwest, rising natural gas dependence, delayed clean energy interconnections, and major transmission constraints are making it harder to add new

[27] North American Electric Reliability Corporation, *Long Term Reliability Assessment*, January 2026, https://www.nerc.com/globalassets/our-work/assessments/nerc_ltra_2025.pdf.

Appendix B. List of Organizations Interviewed

- Center for Grid Security at Securing America's Future Energy (SAFE)
- Consumers Energy Compa
- Jacomb County
- , and Energy (EGLE)
- Midcontinent Independent System Operator, Inc. (MISO)
- Muswell Orange, LLC
- ReliabilityFirst
- Office of Future Mobility and Electrification, Michigan Department of Labor and Economic Opportunity
- The Center for Climate and Security
- United States Army Garrison Detroit Arsenal

Photo Cover Credits: US Marine Corps

THE HIDDEN SECURITY CHALLENGE

Responding to Grid Capacity Constraints and Their Impacts on Military Installations

Nicolette Santos, Master in Public Policy
May 2026

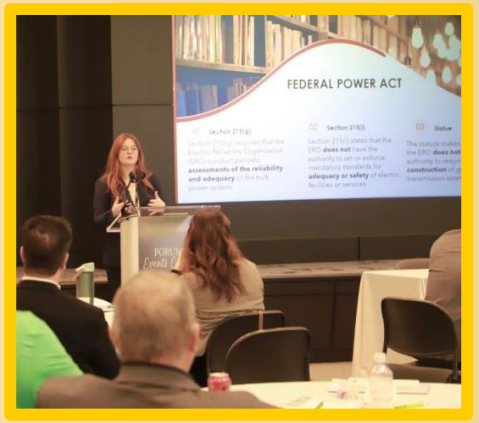
Prepared For: Converge Strategies, LLC
Faculty Advisor: Henry Lee, Jassim M. Jaidah Family Director of the Environment and Natural Resources Program, Belfer Center for Science and International Affairs
Seminar Leader: Thomas Patterson, Bradlee Professor of Government and the Press

Submitted in partial fulfillment of the requirements for the degree of Master in Public Policy. This PAE reflects the views of the author and should not be viewed as representing the views of the PAE's external client, nor those of Harvard University or any of its faculty.

We were interviewed and cited in the Harvard Kennedy School article highlighting the NERC LTRA

RF also presented at the American Council of Engineering Companies Maryland (ACEC/MD) at their 2026 Utilities Seminar in Baltimore (4/16)

Courtney presenting with NERC
(Natural Gas-Electric Coordination)



Catherine presenting at
Indiana Municipal Power Agency

SUSTAINABILITY EFFORTS IN DATA CENTERS FOR AI

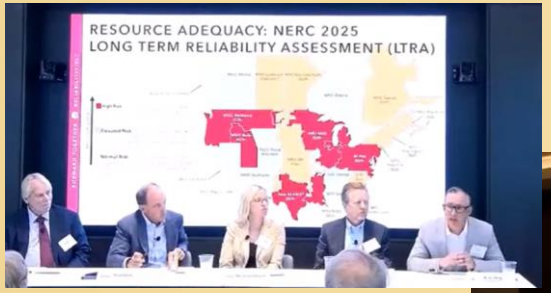
- **DR. BENJAMIN LEE,** PROFESSOR OF ELECTRICAL AND S
  ENGINEERING AND COMPUTER & INFORMATION SCIEN
  UNIVERSITY OF PENNSYLVANIA

TECH TALK WITH RELIABILITY FIRST

Brian and Michelle presented at the Ohio Energy Symposium in Columbus, hosted by the Ohio Chamber of Commerce

RF met with Enbridge, PJM, and FirstEnergy to discuss the interdependencies between the electric and natural gas systems and how those relationships increasingly shape reliability outcomes

RF presented at the Thompson Hine conference, Powering the Future in the AI Age



The session focused on the supply of power for data centers and other major development projects, examining how shifting energy sources, emerging technologies, and evolving regulatory frameworks are reshaping the way organizations plan for and secure reliable power

Coming Soon

RF met with the Pitt Center for Sustainable Business, part of the University of Pittsburgh

Resilient Organizational Architecture Diagnostic (ROAD) Tool

The **Resilient Organizational Architecture Diagnostic (ROAD) Tool** is a propriety tool developed by the CSB in 2024, first piloted in Spring 2025. The tool guides you through our Resilient Organizational Architecture framework to assist you in developing actionable insights for your organization, while also enabling the development of an implementation plan to build your organization's capacity for resilience.

This groundbreaking tool helps you evaluate your organization enabling you to identify, prioritize, and implement strategic interventions to increase your capacity for resilience. Using a systematic framework organized into **22 Key Result Areas**, the CSB developed this tool alongside industry and academic experts based on years of research and practice.

Use the ROAD Tool Now

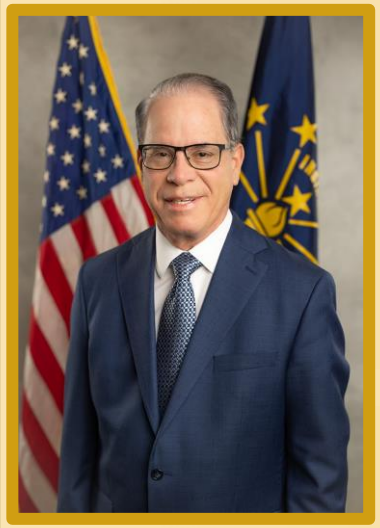
We exchanged ideas, with the CSB sharing their ROAD tool and RF sharing our Community Appraisal program

Building resilience at the community level

ReliabilityFirst can work with cities, villages, or townships in our footprint to assess their readiness, preparedness, and resource strength for long-term disruptions to electrical grid power and other community threats.

We review information generally found in the public domain: city and utility websites, public mass-media records, city council meeting transcripts, etc., and use that to compare a community's abilities, resources, and plans to those of neighboring areas. Ultimately, the goal is to assess, evaluate, and improve a community's ability to organize resources and efficiently survive extended periods without grid power.

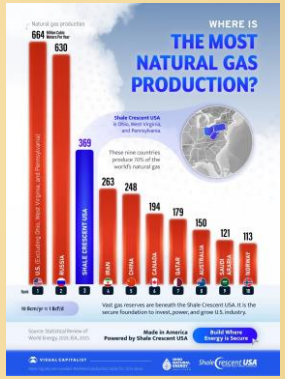
Another option we offer communities is for ReliabilityFirst to facilitate a community appraisal game.



RF met 1:1 with Governor William Braun and Secretary Jaworowski, discussing risks to the Indiana footprint

ARTEX OIL COMPANY

Jerry James (Artex Oil) presented at the RF board meeting



RELIABILITY FIRST

FALL RELIABILITY & SECURITY SUMMIT

SEPT. 14-16, 2026

COLUMBUS, OHIO

Jerry James (Artex Oil) is lined up to be a speaker at the upcoming Fall Reliability Summit this year

2026 MARYLAND CLEAN ENERGY SUMMIT

We met with the Maryland Clean Energy Center twice this year, and will have several members of the state outreach team speaking at their upcoming summit

THE REMAINDER OF THE YEAR

Fall Reliability & Security Summit

September

OMS & OPSI Meetings

October

Follow-up Engagements with Indiana

Various

Maryland Clean Energy Summit

October

PA House Consumer, Technology & Utilities Committee Grid Reliability Roundtable

September

FALL RELIABILITY & SECURITY SUMMIT

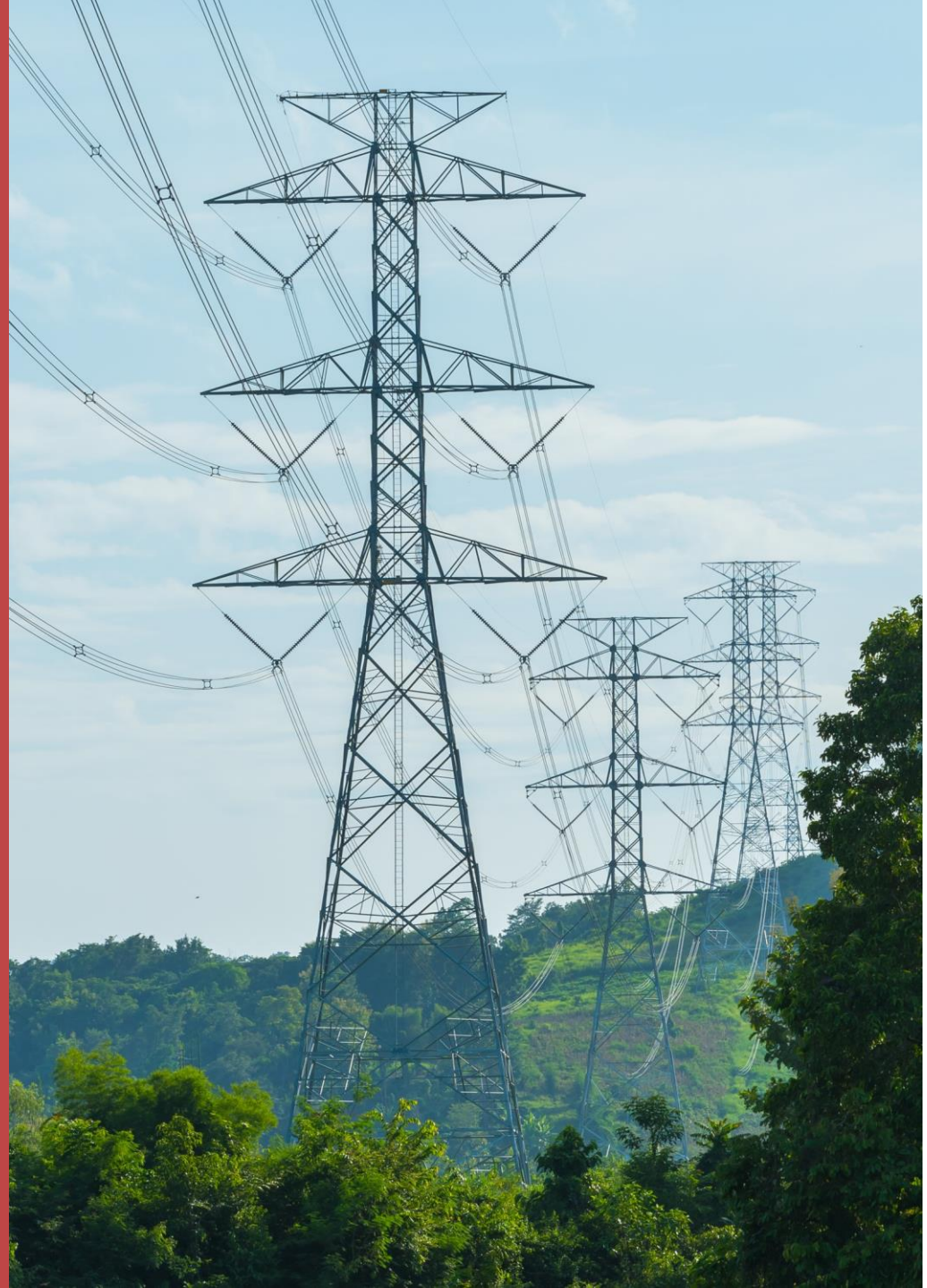
Day 2

Agenda Item
Welcome Message
Keynote Address
RTO Fireside Chat
Data Center Panel
FBI Security Presentation
Natural Gas/Electric Interdependence
Using Data to Mitigate Reliability Challenges
RF Regional Risk Assessment
Awards Reception

Day 3

Breakout Sessions

1. Energy Policy Track
   - Data Centers
   - Energy Assurance
   - Load Flexibility
2. CIP Breakout
   - Cloud
   - Supply Chain (CIP-013)
   - Case Studies from Enforcement
3. Data Submittal Breakout
   - xADS data (GADS, TADS, MIDAS)
   - Self-Reports
   - Event Reporting



QUESTIONS & ANSWERS

Diane Holder

diane.holder@rfirst.org