Joint Supply Chain Practice Group and Supplier Sharing Call

October 6th, 2025 – 2pm-3pm ET

Open Distribution for Supply Chain Materials
Copyright © 2025 North American Transmission Forum ("NATF"). All rights reserved. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use.

Guidelines for this meeting

- This is an open meeting
- Some participants of this meeting are not employees of NATF member companies
  - Do not share confidential information
  - Avoid conduct that unreasonably restrains competition
  - Adhere to your organization's standards of conduct
  - Do not share intellectual property unless authorized

Agenda

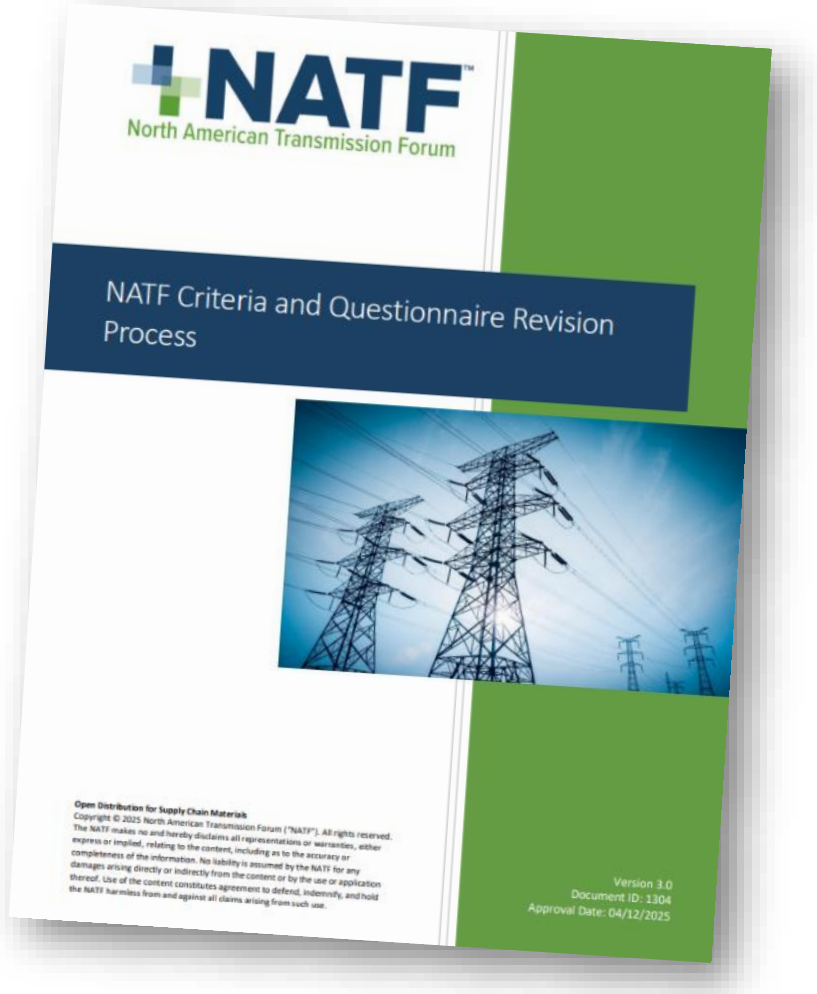
- Supply chain program updates
- Presentation on AI Governance
- Panel on using AI to address supply chain risk

Supply chain program updates

David James Earley, NATF

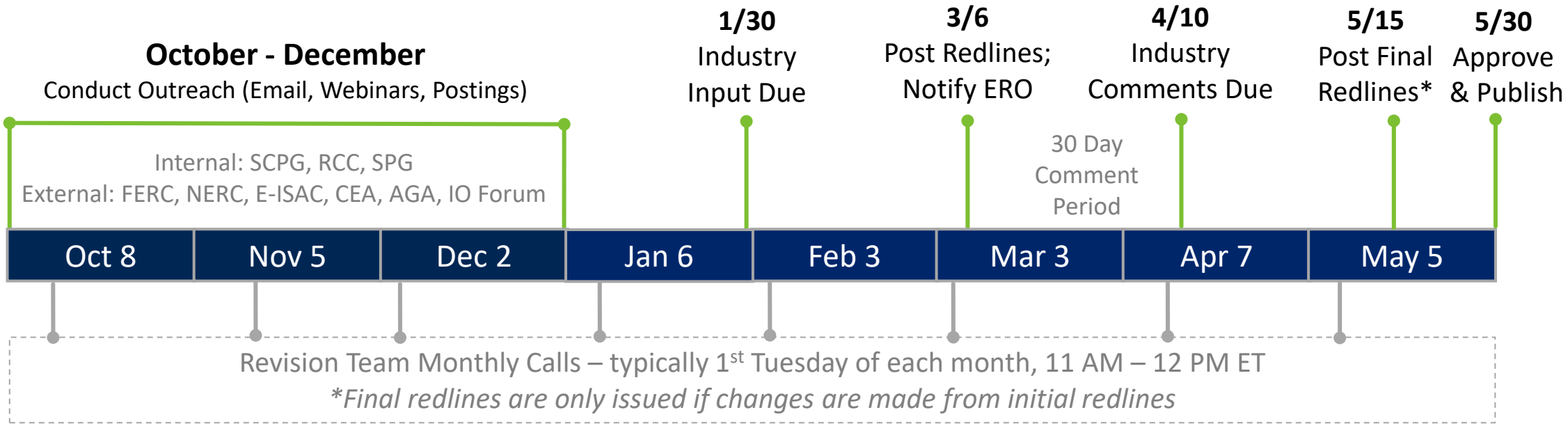
New Criteria and Questionnaire Revision Cycle

- Revision process for 2026 is now open
  - Keeps C&Q updated to industry needs
- Follows published process posted at:
  - https://www.natf.net/industry-initiatives/supply-chain-industry-coordination
- Direct link:
  - https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/natf-criteria-and-questionnaire-revision-process.pdf



Criteria and Questionnaire Revision Update

2026 Annual Revision Process (v7) Timeline



Email proposed changes/feedback to supplychain@natf.net

Questions?

AI Governance

Jonathan Dambrot, Cranium

Open Distribution for Supply Chain Materials
Copyright © 2025 North American Transmission Forum ("NATF"). All rights reserved. Presentations are provided with the presenters' permission for distribution. The NATF makes no and hereby disclaims all representations or warranties, either express or implied, relating to the content, including as to the accuracy or completeness of the information. No liability is assumed by the NATF for any damages arising directly or indirectly from the content or by the use or application thereof. Use of the content constitutes agreement to defend, indemnify, and hold the NATF harmless from and against all claims arising from such use. Further, no liability is assumed for infringement by any presentation materials, artwork, or photographs used in presentations not developed by NATF.

David E.

Today's Presenters

Jonathan Dambrot

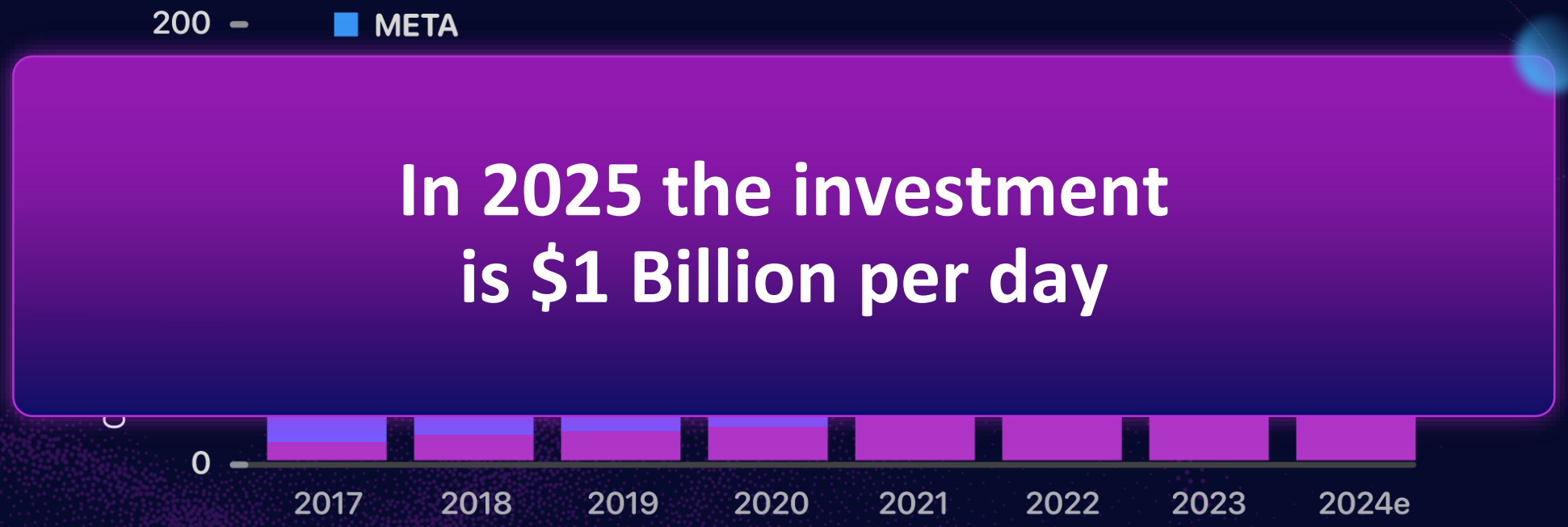
Cranium

CRANIUM

NATF
AI Security & Governance

Supplier Sharing Call
October 6, 2025

Today, 3 Companies are spending **$152 Billion** on AI (2024)



In 2025 the investment is $1 Billion per day

The global (AI) market size **$1.6 trillion by 2030**

CRANIUM

AI Security is lagging as a % of IT spending

Cybersecurity accounts for **5.7%** of total IT spending.

Over five years, this figure has remained relatively stable, ranging from

2% to 11.5%

of total IT budgets*

The percentage of spending varies between industries. Firms in technology sector are leading cybersecurity spend with

9.5%

of their IT budget. In contrast, government spending was the lowest of the sectors surveyed.*

5.7%

of committed AI Capital spending would equal **$57 Billion** in AI Security Spending this year alone.

This is simply not happening…

What we are hearing

GOVERNANCE COMPLEXITY

Manual, fragmented onboarding and review processes that make scaling AI responsibly feel burdensome and difficult to operationalize.

THIRD PARTY & VENDOR RISK

Limited visibility into how vendors are adopting AI, where data is flowing, and whether governance practices are in place.

TENSION BETWEEN SPEED & CONTROL

Desire to innovate quickly while struggling to balance compliance and stakeholder expectations.

AGENTIC AI BEHAVIOR & UNPREDICTABILITY

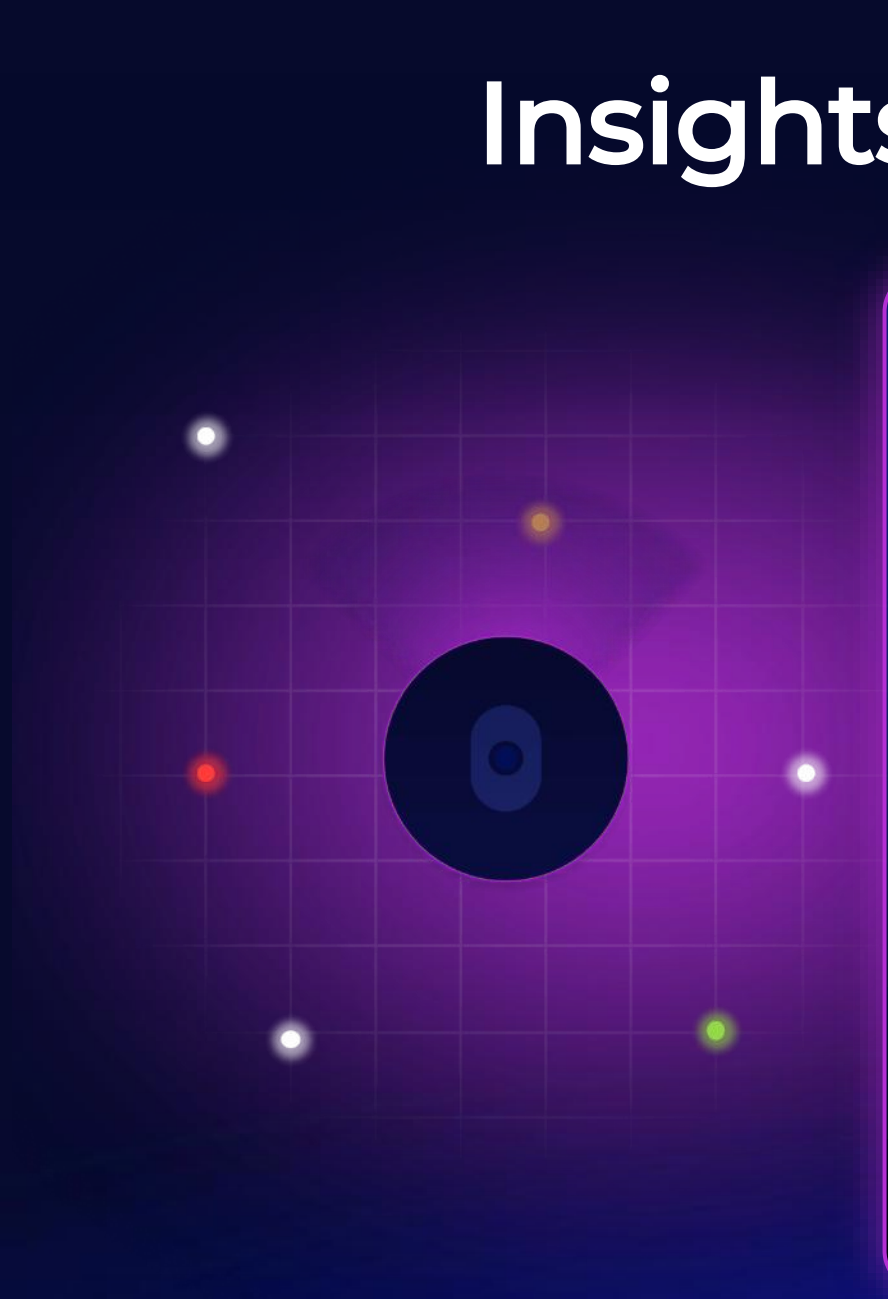
Difficulty managing the output of large language models and autonomous agents – from hallucinations to improper actions in sensitive workflows.

DATA SECURITY & ACCESS CONTROL

Concerns about sensitive data leakage, insufficient access controls, and the risk of exposing customer data through AI features.

CRANIUM

Insights & Leading Practices



What Leading Enterprises Are Prioritizing

- Embedding AI governance into operational workflows
- Aligning with evolving frameworks (NIST AI RMF, EU AI Act)
- Addressing third-party and foundation model risk
- Implementing security-by-design practices across the AI lifecycle
- Conducting AI-specific red-teaming to proactively uncover system vulnerabilities
- Establishing cross-functional accountability to enable faster decisions without compromising oversight

CRANIUM

AI Policy and Implications for Utilities

Evolving US AI Policy Landscape

Federal:

AI Action Plan & EOs
14179 & 14319

Push for **rapid AI adoption** & stronger security, governance, and accuracy standards. Rising expectations for monitoring, adversarial testing, and compliance

CIRCIA

Requires covered entities, including utilities, to **report cyber incidents** and ransomware attacks. Expands federal visibility into AI-related security risks across critical infrastructure.

NIST AI RMF
v1.0 & 600-1

Voluntary but emerging as **de facto standard** for agencies and regulators. Must align AI practices with its principles of governance, monitoring, and trustworthy AI to stay ahead

Regulatory Agency Oversight
DOE, DHS, FERC

Regulators extending oversight in AI & cyber risks. DOE and DHS funding AI for cyber resilience; FERC proposed CIP standards post Volt Typhoon. **Closer scrutiny of AI-enabled monitoring**, anomaly detection, and supply chain defenses.

State:

California
AB 2013, SB 942 & 53

Advancing new **AI guardrails** in effect 2026. Gov. Newsom eager to sign more AI bills. California prioritizing transparency, risk reporting, and safety in AI

Texas
TRAIGA - HB 149

Establishes a regulatory **sandbox program** for developers, the Texas Artificial Intelligence **Advisory Council** and prohibits deployment of AI for certain purposes

Utah
SB 226

Focused on "high-risk" interactions. Requires clear disclosures, creates a **safe harbor** for firms adopting transparency. Maintains an AI Office and sandbox

Colorado
SB 24-205

Imposes duty-of-care rules for **"high-risk" AI,** including disclosures & impact assessments. Delayed due to compliance concerns.

Strengthening AI Guardrails for Utilities

Requirement	Why It Matters
AI Inventory (AI BOM)	Growing expectations for transparency into all AI systems and vendors to uncover hidden risks. Texas law and NIST AI RMF highlight inventories as essential for accountability, especially where third-party SaaS or embedded AI may affect utility operations.
Risk Assessments & Continuous Monitoring	Increasing number of requirements to monitor AI system performance, spotting errors, bias, or security gaps before they cause problems. NIST AI RMF and state AI laws call for ongoing checks across the lifecycle of high-risk AI, making this especially important for grid stability and customer-facing systems.
Adversarial Testing & SbD	Rising pressure to build resilience into AI systems before deployment to prevent misuse or attack. DOE and CISA promote secure-by-design principles, and FERC's CIP-003-11 proposal emphasizes stronger authentication and detection of malicious activity in low-impact grid systems.
Governance & Documentation	Expanding requirements to document how AI systems are designed, tested, and governed to demonstrate fairness and reliability. Colorado's AI Act and California's ADMT rules call for impact assessments, transparency, and audit-ready reporting—critical where AI affects eligibility or customer decisions.
Continuous Protection	Increasing focus on AI-specific incident reporting and rapid response to cyber threats. CIRCIA and DHS/CISA frameworks highlight the need for organizations to maintain forensic logs, playbooks, and continuous protection to respond at machine speed.

Ok, so what should you be doing today?

Do you know where your AI is?

Can you identify AI projects proactively?

Are you investing in your AI Security & Cyber Governance team?

Can you meet your AI Security and Governance Policy internally and with your third parties at scale?

CRANIUM


CRANIUM
Thank You

Questions?

Panel on using AI to address supply chain risk

Mike Pyle, Schnieder Electric
Frank Harrill, SEL
Jennifer Couch, Southern Company

Today's presenters

Mike Pyle

Schneider Electric

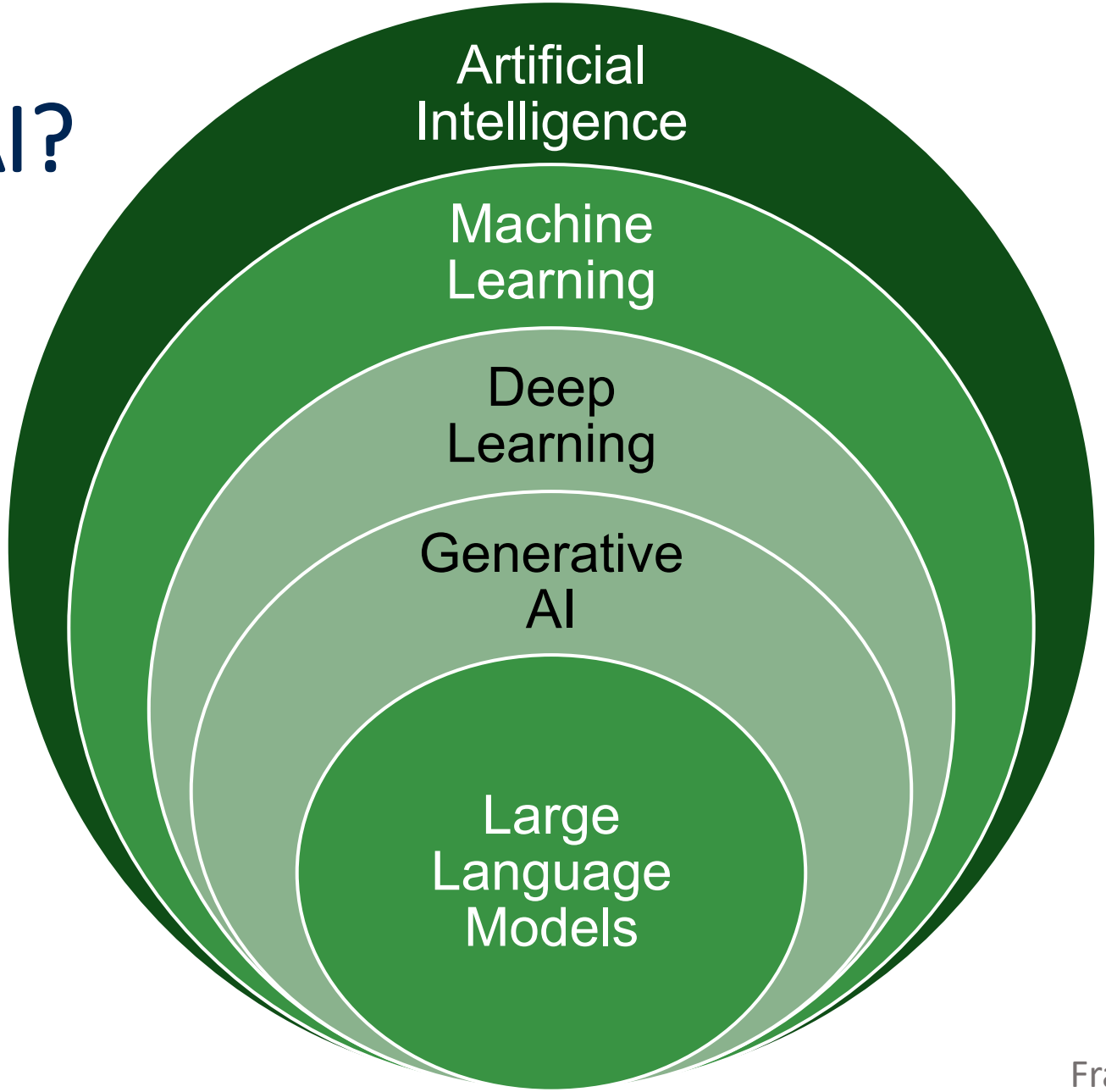
Frank Harrill

Schweitzer Engineering Laboratories

Jennifer Couch

Southern Company

What is AI?



Frank H.

slido

Please download and install the Slido app on all computers you use

Join at slido.com
#3800

ⓘ Start presenting to display the joining instructions on this slide.

slido

Please download and install the Slido app on all computers you use

How are you using AI to evaluate risk posed from your suppliers?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

How are you using AI to aid in responding to requests for information?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

How are you using AI to help create or review contract language?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

What is your company’s appetite for embracing AI?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

How are you using AI? What challenges or opportunities do you see?

ⓘ Start presenting to display the poll results on this slide.

slido

Please download and install the Slido app on all computers you use

Audience Q&A

ⓘ Start presenting to display the audience questions on this slide.

Questions?

Thank you for attending!

NATF Contact Information

NATF Supply Chain - supplychain@natf.net

David James Earley - dearley@natf.net