

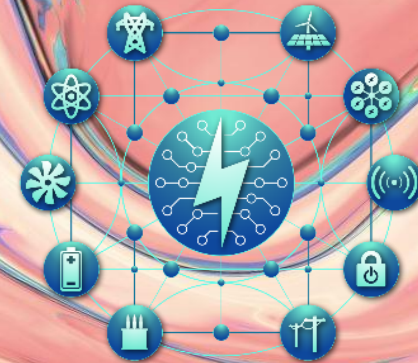
OPAI Consortium™ Data Sharing Working Group

KICKOFF MEETING

DECEMBER 11, 2025

JACQUELINE ROSATI, EPRI

JACK WHITE, EPRI



**OPEN POWER
AI CONSORTIUM**

AGENDA



Introduction

11:00 a.m. Eastern



Classification of Data

11:05 a.m. Eastern



Discussion

11:15 a.m. Eastern



Contractual Templates & Clauses

11:25 a.m. Eastern



Discussion

11:35 a.m. Eastern



Data Protection & Licensing

11:45 a.m. Eastern



Discussion

11:55 a.m. Eastern



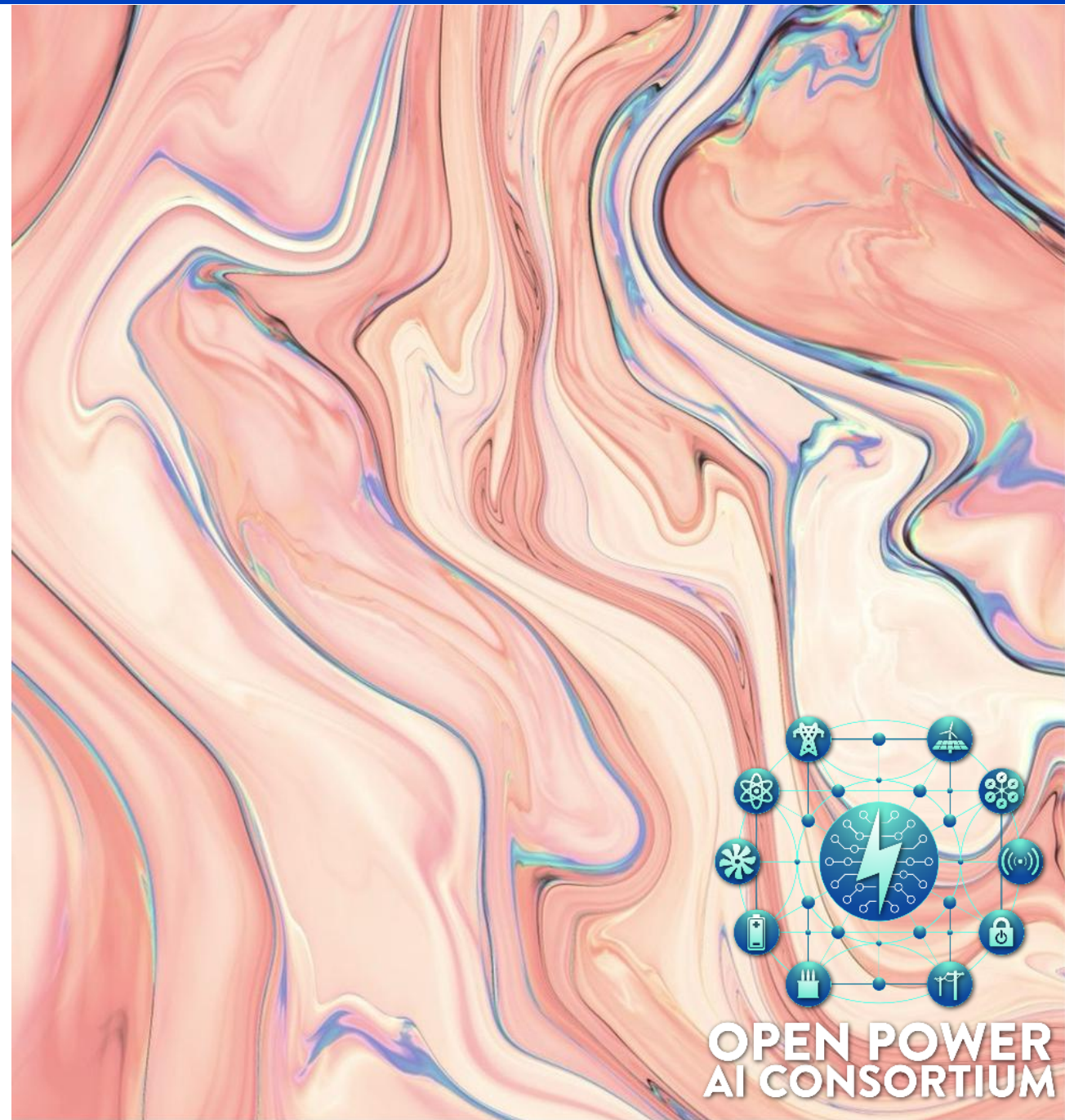
Adjourn

12:00 p.m. Eastern



Introduction

Jacqueline Rosati, EPRI
OPAI Consortium™
Data Sharing Working Group
Kickoff Meeting
December 11, 2025



Working Group Profile

Legal Representatives: OPAI participant representatives with familiarity with participant legal requirements to facilitate data and information sharing to inform OPAI

Cybersecurity Representatives: OPAI participant representatives with familiarity with participant cyber security requirements



WG Leader

10-15
participants



EPRI Corporate Vice President, General Counsel, Chief Compliance Officer & Secretary

Data Sharing Working Group Objectives



Enable Data Sharing

Enable responsible data sharing to support energy-specific AI tool/solution development



Legal Terms

Collaboratively develop contractual templates to facilitate data and information sharing based on type of info. shared. Include security mechanisms appropriate for data and information shared



Security Mechanisms

Define appropriate transmittal, storage requirements. Leverage synthetic data, anonymization and aggregation options



IP Management & Data Security

Through collaboration and innovation, participants will develop and share data and IP specific to common scope. Participants will work together to create and leverage standardized mechanisms to manage data and IP. OPAI is committed to uphold confidentiality obligations and secure data handling.



OWNERSHIP

Each participant retains ownership of its proprietary data and existing IP

PROTECTION

Managed processes for anonymization and aggregation

USE

Clear & standardized agreements: What's shared? What's protected? What's licensed?

THE ROLE OF TECHNOLOGY IN DATA SECURITY



You already do this
with EPRI



EPRI Data
Governance



EPRI
Experience &
Infrastructure



Comfort with
Artificial
Intelligence



Discussion

Classification of Data

Jack White, EPRI

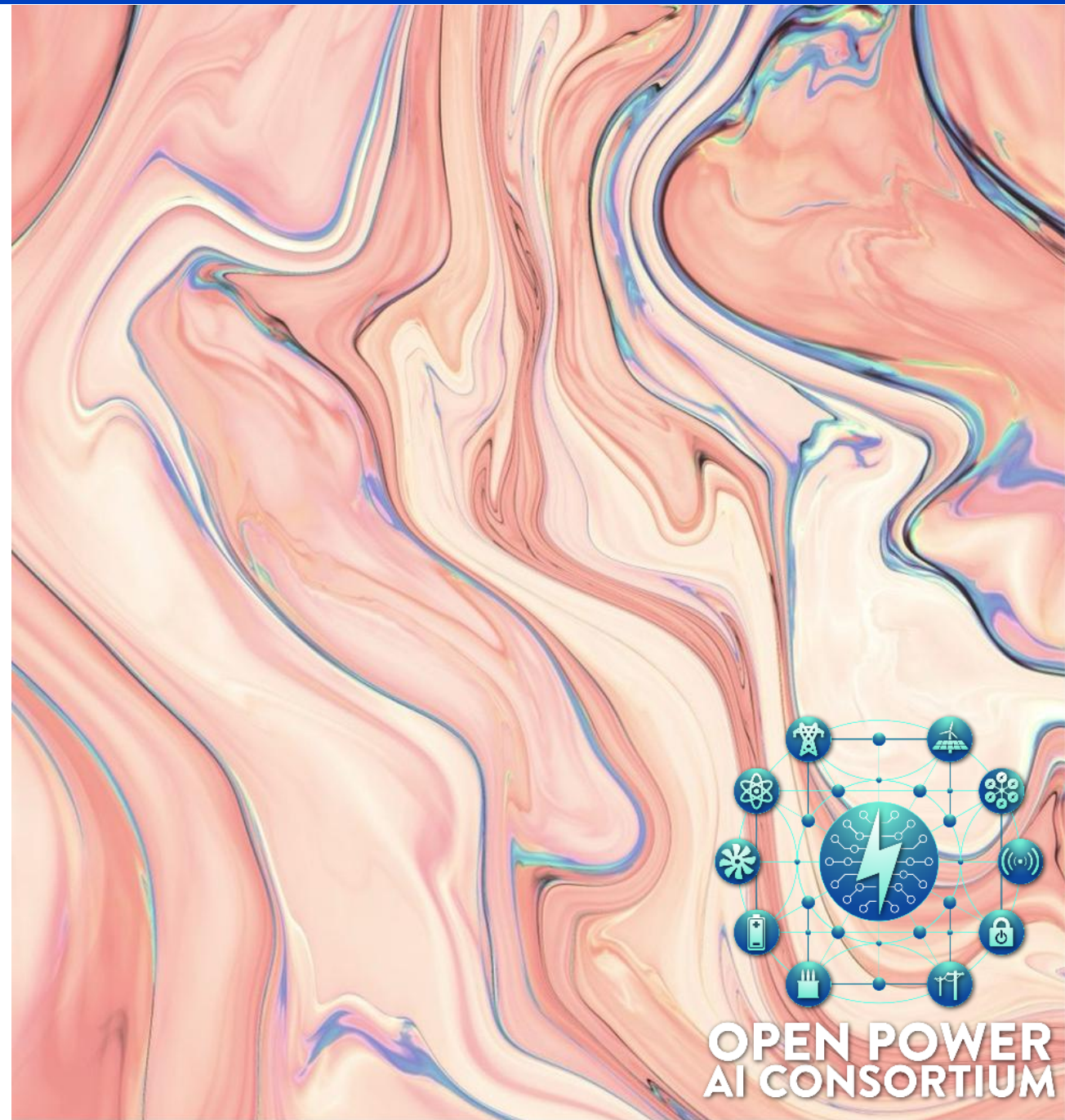
Corporate Counsel I

OPAI Consortium™

Data Sharing Working Group

Kickoff Meeting

December 11, 2025



Classification of Data – What Works?

- Data Classification Schemes & Decision Framework
 - Dataset Ranking – Public, Internal, Confidential, Restricted
- Sensitivity Categories and Legal Implications
 - Data Sensitivities – PII, SEI, ITAR, CUI, 3P IP, Antitrust
- Pain Points with Data Sharing
 - Ownership, Licensing, Reputational Risk, Contractual Requirements and Complexities

Data Classification Decision Tree

RESTRICTED

Contains: PII, ITAR-controlled technical data, CUI (Controlled Unclassified Information), PHI, or material subject to NDA with restriction language

Legal exposure: Regulatory penalties, criminal liability (ITAR), contractual damages

CONFIDENTIAL

Contains: Proprietary business information, SEI (Security Event Information), competitively sensitive data, trade secrets, attorney work product

Legal exposure: Loss of trade secret protection, competitive harm, breach of fiduciary duty

INTERNAL

Contains: Non-public business information, internal analytics, preliminary research data, operational data without sensitivity markers

Legal exposure: Reputational risk, potential competitive disadvantage

PUBLIC

Information already publicly available or explicitly designated for public release

Data Sensitivities – Legal Definitions

PII (Personally Identifiable Information)

Information that identifies or can be used to identify an individual (SSN, name+DOB, biometrics)

Regs: GDPR, CCPA, state privacy laws

SEI (Security Event Information)

NERC CIP-protected data about cybersecurity incidents, vulnerabilities, security systems

Regs: NERC CIP-008, CIP-011

ITAR (International Traffic in Arms Regulations)

Defense-related technical data requiring State Dept. authorization for sharing

Regs: 22 CFR 120-130, criminal penalties

CUI (Controlled Unclassified Information)

Government-created or owned information requiring safeguarding (32 categories)

Regs: 32 CFR Part 2002, NIST SP 800-171

3P IP (Third-Party Intellectual Property)

Data subject to vendor/partner licensing restrictions or confidentiality obligations

Governed by contract terms

Antitrust Sensitive

Competitively sensitive pricing, cost, strategic planning data - improper sharing = antitrust violation

Sherman Act, FTC Act exposure

Pain Points with Data Sharing

- Contractual Liability & Competitive Disadvantage

Contractual Liability Exposure

- **NDA Breaches:** Liquidated damages, injunctive relief, loss of business relationships
- **Data Processing Agreements:** Indemnification triggers for unauthorized use/disclosure
- **Member/Consortium Agreements:** Expulsion, reputational damage, loss of collaborative research rights
- **Vendor Contracts:** License termination, audit rights activation, financial penalties

Competitive Disadvantage

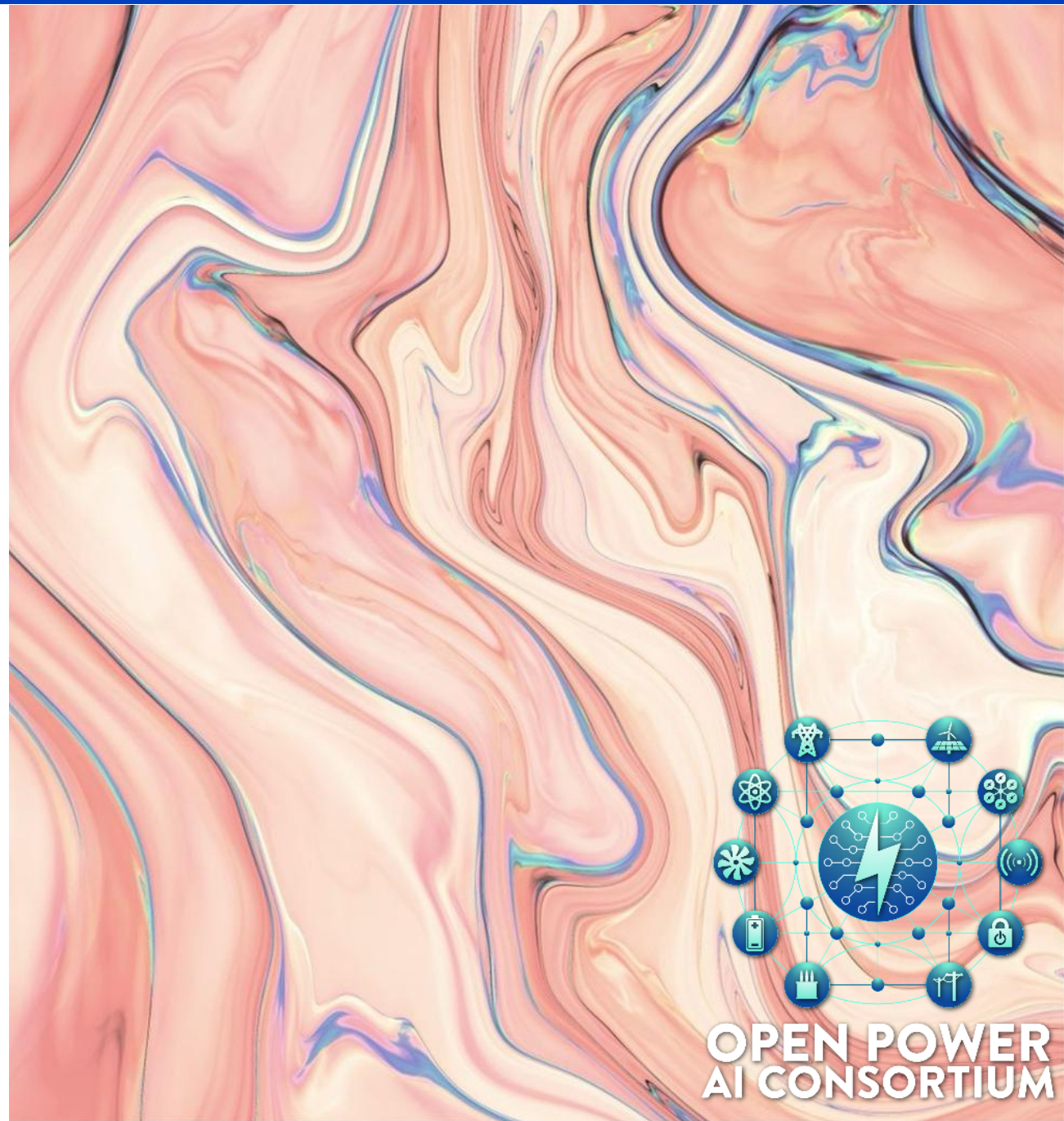
- **Strategic Intelligence Loss:** R&D directions, investment priorities, operational challenges exposed to competitors
- **Pricing Information:** Loss of negotiating leverage; antitrust scrutiny if competitively sensitive data shared improperly
- **Technology Leakage:** Loss of first-mover advantage, reduced ROI on innovation investment
- **Talent Poaching:** Inadvertent disclosure of key personnel, project staffing



Discussion

Contractual Templates & Clauses

Jacqueline Rosati, EPRI
OPAI Consortium™
Data Sharing Working Group
Kickoff Meeting
December 11, 2025



Data Sharing – Outbound to EPRI

OPAI will leverage data to support use cases identified by the OPAI Consortium. There are multiple working groups identifying use cases most valuable to OPAI participants. Surveys have been launched to identify desired use cases and the data needed to support use cases will be prioritized.

OPAI
Contracting

EPRI Members
vs.
Non-members

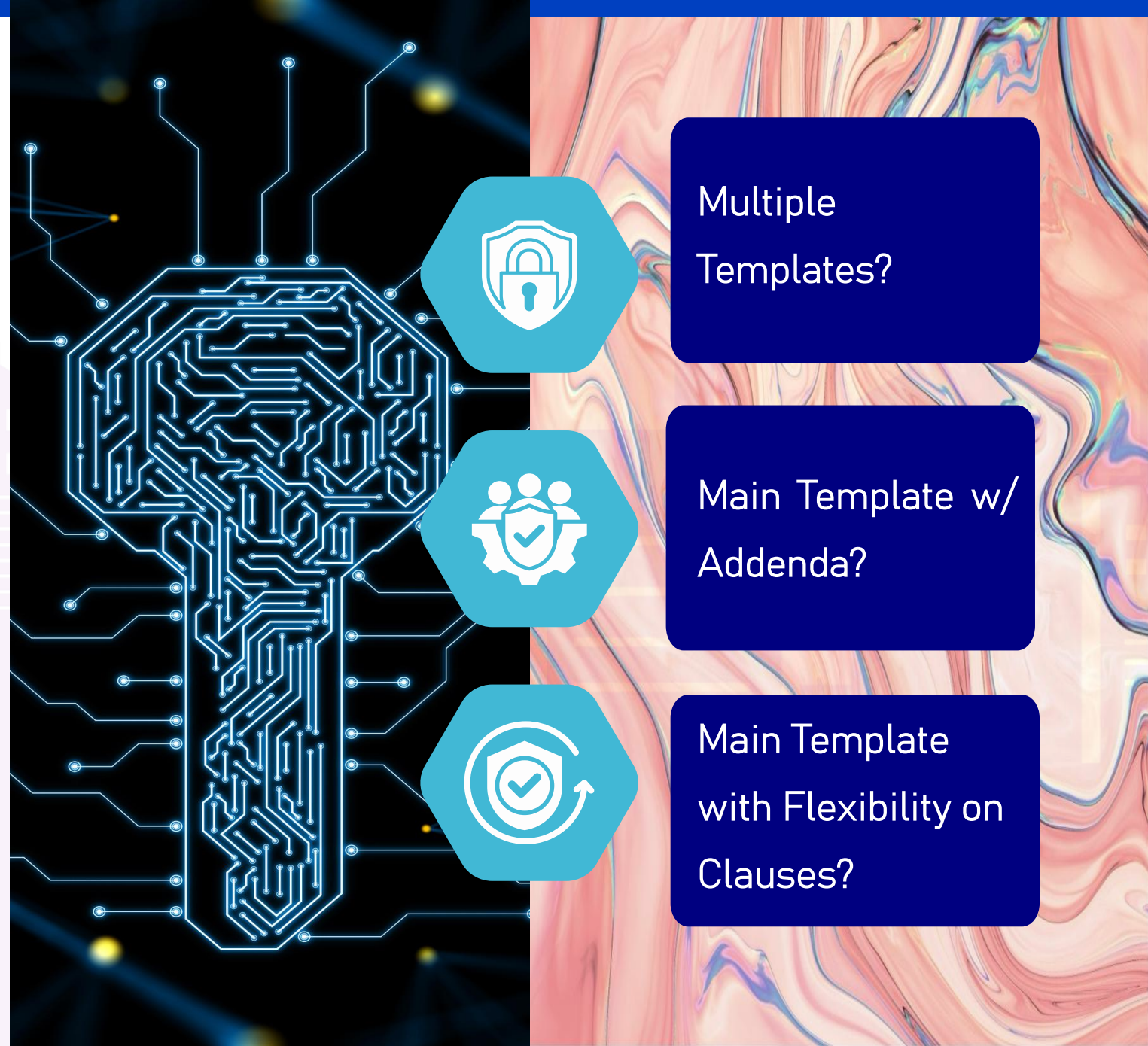
Nature of Data

Transmittal/
Provision of
Data

Structure

The Working Group should discuss efficient ways to contract for and provide data and information to EPRI in support of OPAI Use Cases. Participant data will vary greatly and is key to the success of the OPAI Use Cases.

EPRI will facilitate data sharing while respecting the legal and cybersecurity needs of participants. The Working Group should discuss participant needs to drive a flexible structure for provision and use of data and information. EPRI will provide the first drafts based on such input.

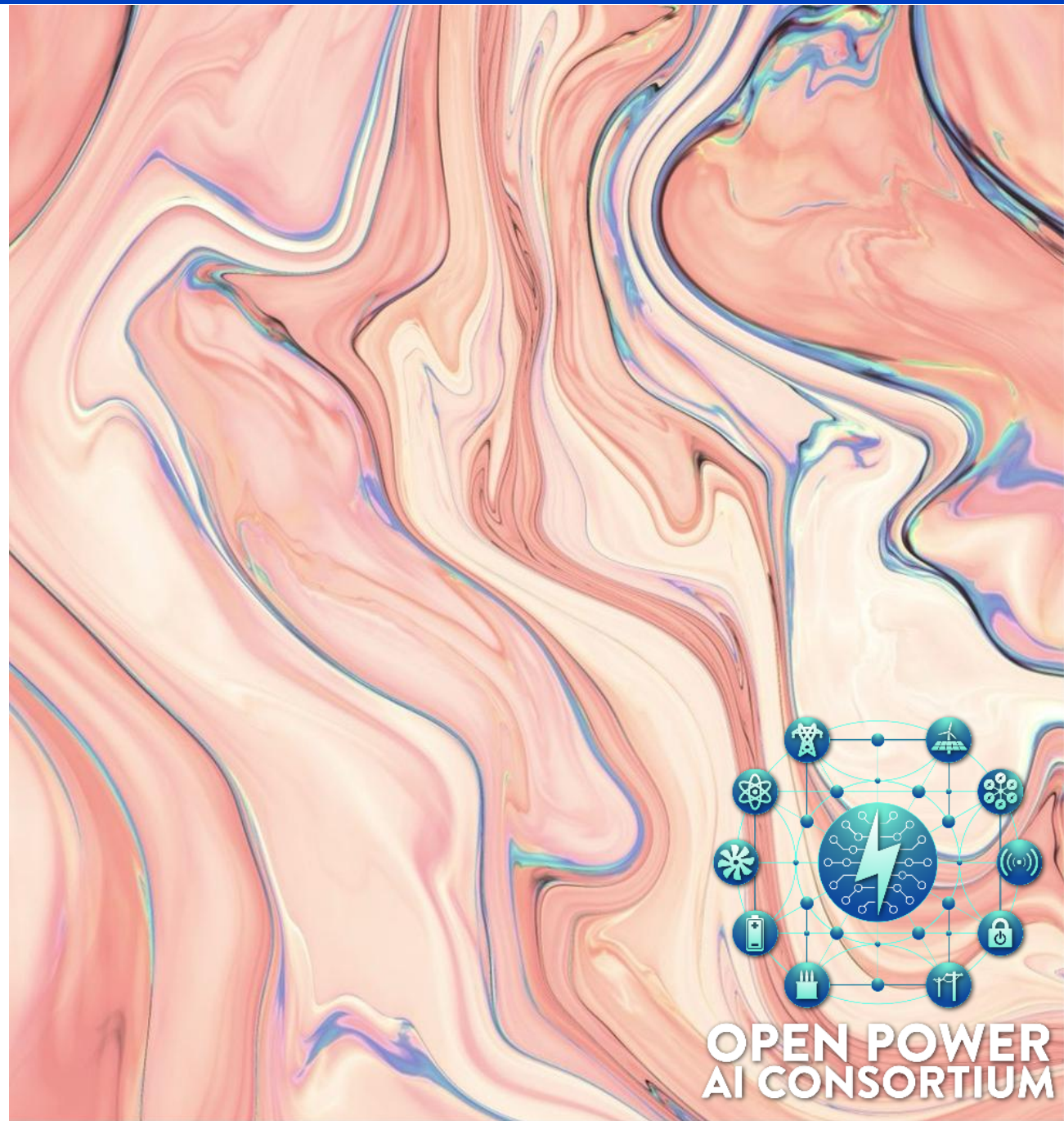




Discussion

Data Protection & Licensing

Jack White, EPRI
Corporate Counsel I
OPAI Consortium™
Data Sharing Working Group
Kickoff Meeting
December 11, 2025



Data Protection and Licensing

- Synthetic Data
 - Tools for generating synthetic data
 - Limitations
- Data Anonymization Techniques
 - Storage Architecture for Privacy Protection
- Licensing Structures for Data Sets

Data Anonymization Architecture

Storage Separation for PII Protection

Separation Strategy: Enabling True Anonymization

By parsing PII into separate storage with different access controls, we can enable legitimate anonymization that survives re-identification attacks

Restricted Zone

Direct Identifiers:

- Names
- SSN/Tax IDs
- Email addresses
- Account numbers
- Device IDs

Encrypted at rest, minimal access, audit logging, separate encryption keys

Controlled Zone

Quasi-Identifiers:

- ZIP code
- Birth date (partial)
- Gender
- Job title
- Equipment types

Generalized/suppressed for k-anonymity, l-diversity testing

Analytics Zone

Non-Identifying Data:

- Aggregated metrics
- Anonymized IDs
- Statistical summaries
- Time-series (coarsened)
- Differential privacy noise

Suitable for research/sharing, survives linkage attacks

Testing Protocols:

- Linkage attack simulation against public datasets
- Mosaic effect assessment
- Quasi-identifier uniqueness analysis
- Differential privacy budget tracking

Data Licensing Structures

Copyright Protection Framework

Legal Foundation: Feist v. Rural Telephone (1991)

"Original selection, coordination, or arrangement" required for copyright protection of factual compilations

Raw facts = not copyrightable | Creative arrangement = copyrightable compilation

Pure Input Data Sets

Raw data collected without creative arrangement

Examples:

- Sensor readings (chronological)
- Equipment serial numbers
- Straight database dumps
- Unprocessed meter data

Copyright Protection: Minimal to None

Protection Via: Contract (NDA/licensing), trade secret (if access controlled), database rights (EU)

Arranged/Created Data Sets

Original selection, coordination, or derived works

Examples:

- Curated research datasets
- Annotated/labeled training data
- Synthetic datasets
- Feature-engineered compilations
- Predictive model outputs

Copyright Protection: Strong (compilation copyright)

Protection Via: Copyright + contract, potential patent (if novel method), trade secret for methodology



Discussion



TOGETHER...SHAPING THE FUTURE OF ENERGY®