DEMARCATION AND OTHER IP-RELATED CLAIMS, INCLUDING IPR

TYPE:	**HIGHLY DISPUTED LANGUAGE**
REQUEST:	**IDENTIFY POTENTIAL IP-RELATED CLAIMS AND CLAIMANTS**
TIMING	**INSTANT; REAL TIME**

A. EXAMPLE REQUEST: Review the Disputed Language and identify all potential Stakeholders, including possible Claims, Claimants, and Parties, no matter how remote.

Vendor	Type	Industry	Document Type:	URL	Potential Stakeholders	Level of Confidence
DOE	AGENCY	GOVERNMENT	Software & Services Agreement (SaaS)	View	R1 Institutions (2), HBCU (2), insurance defense litigation firm (1), cities (2), Members of Congress (2), House Committees (4), Agencies (FCC, NTIA, DIA), banks (1), corporations (C&W plc, Motorola); telecom providers (AT&T, Verizon, Cable & Wireless USA, C&W plc); insurance companies (KP, AIG, CIGNA); cloud-based providers offering SaaS, PaaS, IaaS, UCaaS.	100%

DISPUTED LANAUGE
(VERBATIM)

The language identified below is the focus of several disputes. Instruments containing such language have been flagged as a potential source of uninsurable risk.

VIII.B.16. Nondisclosure and Confidentiality Agreements Representations (June 2015)

By submitting an application in response to this FOA, the Applicant represents that:

(1) It does not and will not require its employees or contractors to sign internal nondisclosure or confidentiality agreements or statements prohibiting or otherwise restricting its employees or contactors from lawfully reporting waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.
(2) It does not and will not use any Federal funds to implement or enforce any nondisclosure and/or confidentiality policy, form, or agreement it uses unless it contains the following provisions:
   (a) ‘‘These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.’’
   (b) The limitation above shall not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.
   (c) Notwithstanding provision listed in paragraph (a), a nondisclosure or confidentiality policy form or agreement that is to be executed by a person connected with the conduct of an intelligence or intelligence-related activity, other than an employee or officer of the United States Government, may contain provisions appropriate to the particular activity for which such document is to be used. Such form or agreement shall, at a minimum, require that the person will not disclose any classified information received in the course of such activity unless specifically authorized to do so by the United States Government. Such nondisclosure or confidentiality forms shall also make it clear that they do not bar disclosures to Congress, or to an authorized official of an executive agency or the Department of Justice, that are essential to reporting a substantial violation of law.

VIII.B.25. Research Misconduct

Recipients are “responsible for maintaining the integrity of research of any kind under an award from DOE including the prevention, detection, and remediation of research misconduct, and the conduct of inquiries, investigations, and adjudication of allegations of research misconduct,” and conducting appropriate administrative processes in response to allegations of research misconduct in accordance with 2 CFR 910.132. Allegations of any misconduct under an award resulting from this FOA must be reported to the appropriate institutional officials in accordance with institutional policies against misconduct. Additional information on DOE research misconduct policies can be found at: https://science.osti.gov/grants/Policy-andGuidance/Research-Misconduct.

VIII.B.26. Rights in Technical Data

Normally, the government has unlimited rights in technical data created under a DOE agreement, including the right to distribute to the public. Delivery or third-party licensing of proprietary software or data developed solely at private expense (“Limited Rights Data”) will not normally be required except as specifically negotiated in a particular agreement to satisfy DOE’s own needs or to ensure the commercialization of technology developed under a DOE agreement.

If software is specified for delivery to DOE, or if other special circumstances exist, e.g., DOE specifying “open-source” treatment of software, then the DOE Contracting Officer, after negotiation with the recipient, may include in the award special provisions requiring the recipient to obtain written approval of the DOE Contracting Officer prior to asserting copyright in the software, modifying the retained Government license, and/or otherwise altering the copyright provisions.

RECOMMENDATION:

FACTS:

The Disputed Language is subject to multiple competing claims, with significant disputes arising among highly skilled and experienced Professionals, generally serving in an advisory capacity, occupying roles such as lawyer, attorney, accountant, consultant, advisor. Such Professionals are the product of top tier educations and have acquired a long list of credentials. They typically work on behalf of some of the World's top Stakeholders, with extensive connections throughout Financial Markets.

OBSERVATONS:

Highly Connected Advisors are reaching exact opposite conclusions regarding key contractual terms arising in contracts and agreements involving cloud-based access to combinations of software, services, platforms, infrastructure, telecommunications, and communications protocols.

Disputes appear to be concentrated at the contract review and negotiation function, with claims arising at the intersection of: (A) intellectual property; and (B) processes variously described as: (1) tech transfer, (2) commercialization, (3) monetization, (4) productization.

These types of contracts and arrangements span multiple roles and functions, including: (1) the General Counsel function (GC); (2) the General Council Office (GCO); (3) cybersecurity; (4) information technology (IT); (5) regulatory compliance; (6) procurement; (7) research and development.

Significant gaps detected at the Federal Research Security Function.

Current arrangements are inconsistent with Open-Source Principles, with negligent adherence to a range of Compliance & Reporting requirements.

Numerous instances of tension, disputes, and gaps surrounding the provision of cloud-based software, services, products, and other solutions.

Using names such as software as a-Service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), and involving access to advanced functions and features (e.g., search and find Menu-like Options), algorithmic functions (e.g., custom embedded prompts), and highly specific, detailed, and precise Metadata, the procurement of such products has resulted in the creation of hidden networks, working "around the clock" on behalf of Unscrupulous Individuals and Entities, each requiring Highly Customized Access to the most sensitive personal data and information.

Instances of such Individuals and Entities engaging in conduct that allows them to essentially "lock" unsuspecting Participants within highly Individualized Custom Environments (generally known as "Simulations" with the people occupying such environments referred to as SIMS).

Unfettered access to Human Data, using Hidden and Closed Networks, has resulted in the creation of an Undesirable, Uninsurable Risk.

CONCLUSION:

An obviously unsustainable structure, especially for Professional Advisors whose job it is to expose such Fake Environments (thus the name “Iron Man”). (Now, do you See?)

Fair fulfilment of the Disputed Language is impossible and, in fact, directly contravenes Open-Source Principles, Protocols, Standards, and Best Practices (“Open-Source Compliance”).

SOLUTION:

It is proposed that the foregoing Risk Anomaly be resolved through the creation of “Retroactive Risk Mitigation” – an AI-enabled Tool designed to access risks in real time and simultaneously create a product that may be offered as a Solution.

PRODUCT:

“Instant Analysis and Real Time Retroactive Intervention,” designed to facilitate Retroactive Risk Mitigation through instant analysis, assessment, and resolution.

METHOD:

Create and send a “Notice of Highly Disputed Language” to each Potential Stakeholder.

MOST EFFICIENT, EFFECTIVE, AND TIMELY OUTCOME:

Instant invalidation of contracts containing such contractual language and the withholding of any funding authorized through the use of such an Instrument.