Synergist Response to NIST RFI
February 2, 2024

Submitted by Elycia Morris CEO Synergist Technologies elycia@synergist.technology, Chris Pernicano CTO Synergist Technologies, Brad Levine CCO Synergist Technologies

On behalf of Synergist Technologies, (www.synergist.technology) we write in response to the National Institute of Standards and Technology (NIST) seeking information to assist in carrying out several of its responsibilities under the Executive Order on *Safe, Secure, and Trustworthy Development and Use of AI* issued on October 30, 2023. We support NIST's efforts in seeking stakeholder input to undertake an initiative for evaluating and auditing capabilities relating to AI technologies and their trustworthiness.

Artificial Intelligence (AI) is revolutionizing several industries, enabling organizations to make data-driven decisions and automate complex processes. However, with the growing complexity and widespread deployment of AI systems, ensuring their trustworthiness has become paramount. Synergist seeks to underscore the reasons why auditing AI is essential to manage risks associated with trustworthiness in a fluid and unprecedented environment. The aspects of trustworthiness such as validity and reliability, safety, security and resilience, accountability and transparency, explainability and interpretability, privacy enhancement, and fairness with the management of harmful biases will be paramount for an organization to assess in real time and longitudinally over time. Synergist Technologies is developing a Software-as-a-Service Platform called, AFFIRM. The AFFIRM platform incorporates emerging guidance from thought leaders like NIST and other global entities trying to set standards for safe and effective AI.

The AFFIRM software addresses a portion of the solution needed around creating trustworthiness in AI from a repeatable, scalable, and cost-effective point of view which in our view is similar to the cybersecurity audits we and others do today. In our research we have uncovered the basic need of inventory as a part of understanding the AI that an organization currently has. In many of our conversations with customers, they report that they are unaware where they have AI as a part of a system they have already implemented. In this case the vendor has added for instance an AI bot/agent or just AI search capabilities to existing systems and either has not been transparent with their customer or has 'buried' the information inside of a framework rarely seen or read by IT departments or risk managers.

We are approaching the audit and compliance of AI systems already built and in-use by governments and organizations with the same rigor and interrogation techniques as a full-scale cybersecurity audit but using very different techniques to uncover AI systems, their data origin and compliance to the ever-evolving standards. Our business model allows us to scale the AFFIRM platform in an efficient and repeatable way so no one state, or organization is taking on the burden of deciding which AI fits with today's standards, knowing tomorrow could uncover another complexity or risk given the nature of AI systems, especially GenAI. AFFIRM offers large and small entities a clearinghouse of sorts to constantly review AI for their constituents, agencies or

shareholders. Once at scale we believe there could be a certificate, potentially government sponsored that establishes which business use cases are ripe for AI and potential AI vendors that deploy safe and trustworthy solutions. In Version 1 of the AFFIRM platform we sought to develop a product that addressed the following:

1. The Role of Auditing AI Systems

   1.1 Auditing Methodologies and Techniques
   1.2 Key Stakeholders in AI Auditing, on-going Process Improvement and Governance

2. Challenges and Considerations in Auditing AI Systems

   2.1 Data Availability and Quality
   2.2 Black Box Nature of AI Systems
   2.3 Scalability and Continuous Monitoring
   2.4 Diverse and Evolving AI Technologies
   2.5 Risk Scoring and Legal Consultations

3. Benefits and Implications of Auditing AI Systems

   3.1 Ensuring Compliance and Ethical Use of AI
   3.2 Enhancing Transparency and Accountability
   3.3 Identifying and Addressing Biases and Harms
   3.4 Building Public Trust and User Confidence

Synergist's Platform of Services including the AFFIRM SaaS

Organizational Readiness for AI:

AI Insight & Action | *Elevating AI Awareness* | *Workforce AI Empowerment*

Our team begins by conducting employee surveys to gauge the current level of AI awareness and proficiency within your workforce. For instance, in a manufacturing setting, these surveys might reveal that employees are primarily familiar with AI-driven automation on the production line but lack awareness of AI's potential in predictive maintenance. Based on these insights, we provide tailored recommendations for factors such as training programs to upskill employees, establishing robust governance frameworks to oversee AI implementations, and fostering a culture that encourages safe AI-driven innovation and collaboration.

AI Awareness & Blind Spot Detection: Do you know where you're using AI?

AI Risk Detection | Blind Spot Illumination | Data Privacy Safeguarding

Unidentified AI systems may inadvertently access and process sensitive customer data, potentially leading to data breaches and privacy violations. Our approach identifies AI engagement across your organization, shedding light on potential blind spots.

Understanding AI Types and Systems:

AI Type Clarity | Bias & Reliability Analysis | Deep AI Insight

We provide insights into the types of AI utilized allowing you to understand the integrity behind the insights. For example, our analysis might reveal the utilization of Natural Language Processing (NLP) algorithms to enhance customer support interactions or Computer Vision AI for image recognition in your e-commerce platform. Synergist goes beyond surface-level awareness by conducting a deep inventory and analysis of the Learning and Language Models (LLM) that your AI systems rely on. This not only helps gauge their reliability but also allows you to pinpoint potential biases or prejudices that may influence decision-making processes.

AI Learning Mode Auditing:

AI Precision Assurance | Risk Tolerance Definition | Tailored Risk Mitigation Strategies

Accuracy Evaluation: Ensuring AI Precision for Critical Tasks: We specialize in assessing the accuracy of AI models for tasks that hold paramount importance to your organization. For instance, in the healthcare sector, we will evaluate the precision of diagnostic AI systems, determining whether the achieved accuracy percentage aligns with industry standards and meets your specific healthcare needs.

Risk Tolerance Analysis: We guide our clients in defining and quantifying your organization's risk tolerance. As example a FinTech client may implement AI for algorithmic trading. Here, we help you establish clear risk thresholds, ensuring that AI-driven trading strategies remain within acceptable boundaries to safeguard your investments and minimize potential financial losses. Our analysis provides valuable insights into risk mitigation strategies tailored to your specific AI applications.

Accountability & Discrimination Checks:

AI Accountability | Ethical AI Practices | Bias-Free Decision Making

We take AI accountability seriously and help you maintain transparency and fairness in AI decision-making processes. For instance, consider an HR department utilizing AI for resume screening. Our proprietary audit function ensures that the AI system is not inadvertently discriminating against candidates based on factors like gender or ethnicity.

We help you uphold ethical standards and prevent discriminatory practices in your hiring processes by providing actionable insights and recommendations.

Synergist would like to thank NIST for their service to our country, the time and energy put forth in soliciting feedback from the public. Synergist seeks to be part of the solution that supports the safe, security and trustworthy development and use of AI.