CYVA Research Corporation Assessed 'Awardable' for Chief Digital and Artificial Intelligence Office's (CDAO) Tradewinds Solutions Marketplace for Further Work in the DoD

PRESS—ARTICLE RELEASE • JULY 1, 2024 09:00 PDT

San Diego, CA – July 1, 2024 – CYVA Research, a cybersecurity innovation, strategic research and development firm today announced that it has achieved "Awardable" status through the Chief Digital and Artificial Intelligence Office's (CDAO) Tradewinds Solutions Marketplace.

The Tradewinds Solutions Marketplace is the premier offering of Tradewinds, the Department of Defense's (DoD's) suite of tools and services designed to accelerate the procurement and adoption of Artificial Intelligence (AI)/Machine Learning (ML), data, and analytics capabilities.

CYVA's internationally patented Personal Information Agent™ & Trust Community (TC) Operator Kit™ innovations (TRL 5 : Not Commercially Available) are dual-use military and commercial technologies designed to provide our Special Operations Forces (SOF) warriors, liberty minded people, communities and businesses worldwide the capabilities to own, protect, control and monetize their personal and business information assets wherever they exist post-decryption; and support the formation and management of ad hoc compartmental smartphone-based Trust Communities (TCs) of PIA™ augmented human and machine entities (IoT). CYVA's Personal Information Agent™ capabilities empower human dignity centric security, privacy and liberty enforced social networking, social media, e-commerce, mobile advertising and emergency medical services.

CYVA's Human Digital Liberty Platforms and Services™ dual-use prototypes include: Personal Information Agent™ (PIA™), PIA Communicator™, Emergency Medical Agent™ (EMA™), Consumer Trusted Ad Agent™ (CTA2™), Merchant Trusted Ad Agent™ (MTA2™), eBazaar™, Trusted Information Utility™ (TIU™) and Personal Information Banking and Brokerage™ (PIB2™) services — CYVA's Augmented Cyber Warrior™ & Trust Community (TC) Operator Kit™ military uses include: modernizing C5ISR-T, HUMINT, information operations, intelligence brokering, irregular cyber warfare, supporting, working with resistance fighters.

CYVA's Personal Information Agent™ innovations are designed to strategically counter foreign and domestic adversaries seeking to destroy America and systematically undermine our American Constitutional values, Bill of Rights, freedom of speech, freedom of thought and religion, right to self-defense, right to create and own property. Our universally recognized human rights are being violated increasingly by techno-authoritarians who have built, own, operate and are expanding the anti-liberty surveillance state. Our human digital existence, our day to day lives, economy, government and society is currently precariously dependent on critical information infrastructure and information technologies that are, at their core: the data object, fundamentally flawed. This fact is evidenced by massive and escalating data breaches and successful cyber-attacks. We are in a cyber crisis with no end in sight.

Big tech surveillance capitalists, the anti-liberty surveillance state and techno-authoritarianism is advancing globally and dependent on a primitive-weak dumb data object paradigm and status quo to maximize their mass collection, exploitation and control of humans everywhere. Our data is weak, vulnerable, easy prey. This is by big tech design. CYVA argues it is time to re-engineer cyberspace at its core: the data object which is the fundamental and purposeful flaw being exploited by big tech and techno-authoritarians such as the CCP who wage unrestricted hybrid warfare and mass collection and exploitation of our personal, corporate and governmental information assets.

Techno-authoritarians and profit-power driven surveillance capitalists do not want humans to be able to own, protect, control and license-monetize their digital identities and personal information assets. Control of our personal information is essential to their profits and tyrannical power.

CYVA's video, Augmented Cyber Warrior & Trust Community (TC) Operator Kit, accessible only by government customers on the Tradewinds Solutions Marketplace, presents the company's prototype Personal Information Agent™ (PIA™) and Trust Community (TC) Operator Kit™. CYVA's Personal Information Agent™ is an owner-operator controlled, intelligent (Safe White Box AI™), self-protecting, self-governing, self-monetizing mobile identity agent (HW/SW). The PIA™ provides, augments people, SOF cyber

warriors (dual-use) and communities with the capabilities to own, protect, control and license-monetize their digital identity and information assets wherever they exist post-decryption. We call this Human Digital Liberty™. These capabilities are the foundation in forwarding disruptive innovative approaches to the challenges of security, privacy, and liberty in our presently hostile cyberspace as conceived, supported and engineered by techno-authoritarians and anti-liberty surveillance capitalists.

It is critical our SOF warriors and citizens have the capabilities to own, protect, control and license-monetize their identities and information assets e.g., pictures, messages, target data, geo-location, identity attributes wherever they exist post-decryption across hostile environments and distributed domains. Cyberspace is a domain of war. All of us are being surveilled online, our SOF warriors and their families have long been priority targets for our enemies (CCP, Russia, NK, Iran) who have skillfully exploited our fundamentally flawed data fabric, our presently, by design, primitive-weak dumb data that were never designed to be owner-operator controlled, intelligent (Safe White Box AI™), self-protecting, self-governing, self-monetizing.

CYVA Research was recognized among a competitive field of applicants to the Tradewinds Solutions Marketplace whose solutions demonstrated innovation, scalability, and potential impact on DoD missions. Government customers interested in viewing the video solution can create a Tradewinds Solutions Marketplace account at tradewindAI.com.

Security Rule #1: Trust No One

Always maintain control of your data wherever it exists e.g., lock-at-will, erase-at-will, audit-at-will. Especially do not trust anyone or organization that does not respect the right of people to own, protect, control and license-monetize their personal information assets wherever they exist, does not respect, support and defend the U.S. Constitution, Bill of Rights, and a strong military.

Our Escalating Cybersecurity Catastrophe is Entirely Manmade

OPM Data Breach 22.1 Million SF-86 files stolen by China's Ministry of State Security 2014-2015

Over 2.6 billion personal records were breached in 2021 and 2022 (1.1 billion in 2021 and 1.5 billion in 2022)

According to FBI since January 1, 2016 more than 4,000 ransomware attacks have occurred daily. Encryption Used Against Us

The CCP uses TikTok to "track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."

Data breach victims top 1 billion in 2024's first half. Here's why.

There is no end in sight to successful cyber-attacks and data breaches with devastating impact. Why? At the core of this unending cyber catastrophe is data. Our data is weak, vulnerable, easy prey. This is by big tech design. Data can be used for us (good) and against us (evil). We presently have little if any control over domestic: big tech and big government and foreign: CCP mass collection and exploitation of our, by design primitive-weak dumb data, our human digital existence.

SOF owner-operators and citizens should be equipped to always maintain direct authoritative data custody-control of their identities and information assets across all domains. How is this achieved? SOF owner-operator and citizen authored security rules governing access, processing and exchange of their identities and information assets are encapsulated with and travel with their dispatched Personal Information Agent™ and continuously enforce SOF owner-operator, citizen chosen policies on confidential computing, Trusted Execution Environment (TEE) capable processors (HW/SW). Respect and never separate a person's data from their governing rules: Human Digital Dignity™, Human Digital Integrity™ architecture principles. In addition, Trust Community (TC) member trust reputation management is real-time and dynamic as necessary in war and life in our presently hostile cyberspace.

Going Beyond Encryption

Encryption works well for hiding the meaning of a message but we need to go beyond hiding the meaning and continuously control the message or any data post-decryption. We need to operationally control, control the operations on data objects post-decryption, such as display, read, update, delete, execute, play, exchange and encrypt. Once primitive data is encrypted confidentially and integrity can be protected, provided the encryption scheme is properly implemented. However, once primitive data is decrypted, a key is provided to the recipient for decryption, you are at the mercy of recipients and systems in safeguarding and controlling access to and use of these primitive data objects post-decryption. Recipients of primitive data objects can do whatever they want with the decrypted data.

SOF operators, liberty-minded citizens should be able to operationally control: lock-at-will, erase-at-will, audit-at-will, change governing security and privacy policy-at-will of their personal information assets (messages, pictures, target data, geo-location, identity attributes) wherever it exists. Having the cyber warfare capability to leave no digital footprint, no digital trail for adversaries to exploit is a critical capability for many SOF operators and operations as affirmed by USSOCOM and USASOC SOF warriors. Modernizing C5ISR-T, information operations, HUMINT, irregular cyber warfare operations is critical.

Strategically Countering Globalists' Assault on American Constitutional Values and the Anti-Liberty Surveillance State

The primitive-weak dumb data paradigm and status quo is necessary for big tech's anti-liberty surveillance capitalist business model and continued maximum collection and exploitation of our personal information for profit, assuring tyrannical big government, and unrelenting globalists' assault on American Constitutional values. Information is power, the power to manipulate, coerce, intimidate, cancel and kill. Unchecked and pervasive surveillance powers to track, profile and continuously monitor humans are critical to techno-authoritarians determined to maintain coercive and oppressive control over populations.

The war over who owns and controls our personal information has raged for years and we, the people, are the losers as big tech and big government lawmakers and agencies have proven unequivocally hostile to privacy, informational self-determination, the unalienable human and human digital rights of people everywhere to own, protect, control and monetize their information assets. We all have a human digital existence. Unfortunately our human digital person, is by design weak, vulnerable, easy prey.

Humans worldwide should be empowered, augmented and equipped to own, protect, control and license-monetize their personal information wherever it exists. And if anyone should be monetizing our data it should be us or our chosen trustworthy custodians who respect and defend our human digital rights and not big tech, and a sea of data brokers, human digital traffickers who are callously indifferent to human security, privacy and liberty.

Security + Privacy = Liberty

Security - Privacy = - Liberty: Anti-Liberty Surveillance State

Can we control our data wherever it exists? No. Can data protect itself. No. Is data intelligent? No. CYVA has applied first principles thinking and re-engineered primitive-weak dumb data, creating a new class of data objects (HW/SW) that are owner-operator controlled, intelligent (Safe White Box AI™), self-protecting, self-governing, self-monetizing. Our Personal Information Agent™ (PIA™) and Human Digital Liberty Platforms and Services™ technologies are highly disruptive innovations.

Scientific and engineering breakthroughs and new paradigms take time in terms of market adoption and new industry creation. Breaking up big tech is possible however our lawmakers are far too corrupt and owned by an industry far too rich and powerful. Encouraging, augmenting, equipping and training people to take control of their personal information realizing their security, privacy and liberty depend on it will be accelerated as the actual loss of freedoms, censorship and persecution by techno-authoritarians will fuel widespread resolve and action.

Historical Analogy: Our Auto Industry Then, Our Information Technology Industry Today

Unsafe at Any Speed: The Designed-In Dangers of the American Automobile authored by Ralph Nader and published in 1965 documented the designed-in dangers of automobiles. Our U.S. auto manufactures built cars for 85 years without safety belts being standard equipment. Thousands died.

Today: Our data has no safety belts. This is by big tech design.

Unsafe at Any Clock Speed: The Designed-In Dangers of Information Technology would be an appropriate title for a new book calling out our present by design fundamentally flawed information technology reality. Our by design weak, vulnerable, easy prey, dumb data is being used against us, not for us. Big tech's willful negligence and undermining of disruptive cybersecurity, privacy and liberty innovations that provide humans the capabilities to own, protect, control and monetize their personal information assets needs to be addressed by authorities but too much of our government is controlled by corrupt politicians and agencies.

Millions of people and businesses suffer the consequential cybersecurity, cyberterrorism, privacy, and liberty harms every day. Nader's book was a catalyst for much needed change in automobile safety. "The book became an immediate bestseller, but also prompted a backlash from General Motors (GM), which attempted to discredit Nader."

AI Differentiation: Safe, Verifiable, Reliable, Human Understandable, Controllable, Trustworthy and Maintainable AI Systems

CYVA's Personal Information Agent's AI 'white box' rule engine, code generation and maintenance capabilities are highly valuable and necessary in supporting a safe, verifiable, reliable, human understandable, controllable, trustworthy and maintainable security, privacy and liberty code logic that governs AI enhanced PIA™ behavior and PIA™ to PIA™ interactions. People, human operators will author, instruct, and train their Personal Information Agents that are designed to always enforce the human owner-operator's security, privacy and liberty policies wherever their PIA™ exists. PIA™ dual or multiple owner-operators are supported as law enforcement, parent-child, elder care custodian, corporate, organizational and governmental agency policy can require.

PIA™ owner-operators choose and set their rules governing display, read, lock, erase, audit, emergency access, update security and privacy rules, store, encrypt, execute, play, exchange, license-monetization of their personal information assets. We encourage people to never sell their data, their information assets, but license those information assets according to their terms and conditions; and always authoritatively directly control those assets wherever they exist post-decryption. Lock-at-will, erase-at-will, audit-at-will, update security, privacy, and license-monetization policy-at-will are examples of PIA™ operational control over deployed information assets contained within the owner-operator's mobile PIA™.

Rules governing our personal information assets, our human digital existence can become complex. CYVA is utilizing AI 'white box', safe, human understandable algorithms (enhanced ID3) to guide, generate and maintain rule-code quality, security and reliability with rule conflict detection. The rule generator, used all the way down to program logic, points out contradictions in rule and code logic as well as indicating logic areas that need to be added/enhanced, guiding development and maintenance. Our PIATalk™ language is robust in capturing security, privacy and liberty rules in a human understandable manor contrasted with a complicated neural networks 'black box' AI approach that we don't really understand exactly how they work, make a decision. We contrast this with a human understandable decision tree 'logic' wherein the security logic can be understood, documented, traced and affirmed.

It is critical we address AI 'knowable good use of our personal data for us' v. AI 'unknowable potentially evil use of our personal data against us'. Can complicated neural networks that have learned our geo-location, facial and other biometrics be trusted not to use this information against us, to oppress, intimidate, censor, hunt and kill us? How do you unlearn large models, a vector space, an AGI or superintelligence that knows us, that has been trained with our presently always-on surveilled human digital and physical existence, our data? Will AGI simply pretend to not know our data any longer? These concerns: right-to-be-forgotten, unlearning private and copyrighted data are being worked on, see Machine Unlearning in 2024, by Ken Liu, May 2024.

We presently have very little if any control of our data, the mass collection, exploitation and expansion of the anti-liberty surveillance state. This is by big tech design. There is great AI potential for good but also unknowable and vast evil.

John Lennox on "2084: Artificial Intelligence and the Future of Humanity"

"But as soon as it gets really complicated, we don't actually know what's going on any more than we know what's going on in your brain...we designed the learning algorithm... But when this learning algorithm then interreacts with data, it produces complicated neural networks that are good at doing things. But we don't really understand exactly how they do those things...one of the ways in which these systems might escape control is by writing their own computer code to modify themselves. And that's something we need to seriously worry about..." Geoffrey Hinton 'Godfather of AI' CBS Interview Oct 8 2023

CYVA Research Guiding Architecture Principles: Human Digital Dignity™ and Human Digital Integrity™

A person's unalienable rights of free speech, freedom of thought, informational self-determination, self-defense, freedom of religion and right to create and own property should be respected in both the physical and cyberspace domains. Our guiding architecture principles of Human Digital Dignity™ and Human Digital Integrity™ are foundational to our PIA™ technology designed to support and defend our American Constitutional values in cyberspace which are under determined assault by our anti-liberty authoritarian enemies. It is strategically critical to our shared liberty and cyberwar fighting capabilities we re-engineer primitive-weak dumb data objects to be owner-operator controlled, intelligent (Safe AI), self-protecting, self-governing, self-monetizing.

Irregular Cyber Warfare: A Strategic View

Our present cyber battlespace agility and dominance is negatively affected by the primitive-weak dumb data paradigm promoted by big tech and exploited all day long by our enemies (CCP, Russia, NK, Iran,…) and the tyrannical anti-liberty surveillance state.

Adapting, improvising, and moving strategically to overcome these inherent data weaknesses will require new thinking, new approaches.

Strategically we need to re-engineer cyberspace at its core: the data object to be owner-operator controlled, intelligent (Safe White Box AI™), self-protecting, self-monetizing. This is critical to human security, privacy, and liberty worldwide and our cyber warriors being fully equipped to conduct irregular cyber warfare.

We must revise, re-engineer the cyber battlespace to our advantage. We should equip and empower liberty-minded and purposed peoples worldwide to not only survive under tyranny but thrive in their pursuit of liberty and inalienable rights: freedom of ideas, speech, conscience, religion, self-defense, property, and privacy: informational self-determination.

Superintelligent AGI Unknowability, Potential Good and Evil

There is much concern with superintelligent AGI 'black box', unknowable neural network technology. The accelerating AI deep learning capabilities, AIs training themselves and writing their own code is very concerning. Misaligned superintelligent artificial general intelligence (AGI) is rightfully concerning and many AI scientist such as Geoffrey Hinton and others are voicing their concerns: AI 'godfather' Geoffrey Hinton warns of dangers as he quits Google, 2 May 2023, Zoe Kleinman & Chris Vallance, BBC News. Additional reading: Elon Musk says Larry Page no longer a 'close friend' following AI dispute.

CYVA Research, based on information and belief affirms these AGI concerns and is laboring to address these dangers and the use of our personal information against us and not for us by techno-totalitarian regimes, systems, people, whether AI-based or not. We are utilizing safe, verifiable, reliable, human understandable, controllable, secure, trustworthy and maintainable 'white box' AI algorithms and technology for the purpose-built, principled development of human dignity centric security, privacy and liberty capabilities. We are augmenting humans and institutions committed to faithfully support and defend our American Constitutional values, our Bill of Rights and universal human rights shared and respected by compassionate, just and liberty minded peoples everywhere, all life, liberty, and prosperity minded nations.

###

About CYVA Research Corporation: CYVA Research is a cybersecurity innovation, strategic research and development firm. Our focus is developing disruptive security, privacy and liberty technologies and strategies for our clients. CYVA's internationally patented Personal Information Agent™ (PIA™) technology is an owner-operator controlled, intelligent (Safe White Box AI™), self-protecting, self-governing, self-monetizing mobile identity agent (HW/SW). The PIA™ provides, augments people and communities with the capabilities to own, protect, control and license-monetize their identity and information assets wherever they exist post-decryption. We call this Human Digital Liberty™. These capabilities are the foundation in forwarding disruptive innovative approaches to the challenges of security, privacy, and liberty in our presently hostile cyberspace.

CYVA Research's Augmented Cyber Warrior & Trust Community (TC) Operator Kit video achieved "Awardable" status on July 1, 2024 through the Chief Digital and Artificial Intelligence Office's (CDAO) Tradewinds Solutions Marketplace. Video can be viewed here at: https://cyva.com/videos/tradewinds/CYVAResearch_AugmentedCyberWarrior_TC_OperatorKit5Min.mp4

YouTube: https://youtu.be/ninmO6WPPrw

On Rumble: CYVA Research Augmented Cyber Warrior™ & Trust Community (TC) Operator Kit™ (rumble.com)

Personal Information Agent™ (PIA™) Prototype Video (10 minutes): https://www.youtube.com/watch?v=sCJUAccJUyk

(4 minutes) : https://youtu.be/ZschEW5iLQg

For more information or media requests, contact: Kevin O'Neil, info@cyva.com

About the Tradewinds Solutions Marketplace: The Tradewinds Solutions Marketplace is a digital repository of post-competition, readily awardable pitch videos that address the Department of Defense's (DoD) most significant challenges in the Artificial Intelligence/Machine Learning (AI/ML), data, and analytics space. All awardable solutions have been assessed through complex scoring rubrics and competitive procedures and are available to Government customers with a Marketplace account. Government customers can create an account at www.tradewindai.com. Tradewinds is housed in the DoD's Chief Digital Artificial Intelligence Office.

For more information or media requests, contact: Success@tradewindai.com