Federal Register Notice 86 FR 46278, https://www.federalregister.gov/documents/2021/08/18/2021-17737/request-for-information-rfi-on-an-implementation-plan-for-a-national-artificial-intelligence, October 1, 2021.

Request for Information (RFI) on an Implementation Plan for a National Artificial Intelligence Research Resource: Responses

September 21, 2021

VIA ELECTRONIC SUBMISSION

Re: Request for Information (RFI) on an Implementation Plan for a National Artificial Intelligence Research Resource

Infiltron is a Veteran-owned cybersecurity startup, focused on delivering proactive, real-time Internet-of-Things security solutions and improving biometric protection, fraudster detection, and malware intrusion for IoT devices. It leverages artificial intelligence (AI) technology, among others, to provide innovative cybersecurity protections.[1] Infiltron appreciates the opportunity to submit these comments to the National Artificial Intelligence Research Resource (NAIRR) Task Force.

Ethical, responsible, and fair development and deployment of AI technology (including democratizing access to AI research and development) needs to start at the top, with the government setting the right tone and parameters at multiple levels. The government has a vital role in creating legislation and regulation that holds companies accountable for responsibly developing AI technology.[2] As a customer, the government should expect its vendors to develop good technology rooted in good data. And—of particular relevance when it comes to the work of the NAIRR Task Force—the government can help startups access the quality data and resources they need to develop cutting-edge, responsible technology.

Infiltron seeks to hold itself accountable in developing responsible technology, for example through focusing on the accuracy of facial recognition data and AI trustworthiness. In addition to our responses to the questions posed, the NAIRR Task Force may be able to learn from Infiltron's experience, as noted below.

---

[1] Infiltron, https://infiltron.net/.

[2] For example, the Algorithmic Accountability Act considers how to combat bias in AI, protect the security of people's personal information, and monitor the accuracy and use of that data. *See* Press Release: Booker, Wyden, Clarke Introduce Bill Requiring Companies to Target Bias in Corporate Algorithms (Apr. 10, 2019), https://www.booker.senate.gov/news/press/booker-wyden-clarke-introduce-bill-requiring-companies-to-target-bias-in-corporate-algorithms. Infiltron has been involved in advancing similar state-level legislation in Georgia.

--

Response to Question 1. What options should the Task Force consider for any of roadmap elements A through I above, and why?

> *A. Goals for establishment and sustainment of a National Artificial Intelligence Research Resource and metrics for success;*

As noted above, startups need access to quality data and resources—the fundamental building blocks that will allow them to participate in developing cutting-edge, responsible AI technology. The NAIRR should be developed in a way that permits startups and other researchers access to multiple, unbiased data sets; that instills best practices across the innovation ecosystem; and that incorporates ethical norms during education and training.

> *C. A model for governance and oversight to establish strategic direction, make programmatic decisions, and manage the allocation of resources;*

Diverse representation in the NAIRR's governance will be critical to the development of fair, equitable, unbiased technologies. Diverse leaders should shape the NAIRR's strategic direction, programmatic decisions, and allocation of resources. We know that diversity leads to better outcomes. Ensuring a broad set of stakeholders have a seat at the table will help the resource be dynamic and responsive to future developments and promote development of ethical, trustworthy AI. To this end, the Task Force should consider the importance of diverse representation along several lines—racial, ethnic, gender—as well as type of stakeholder—including startup founders or members of the startup ecosystem, academics, researchers, and others.[3]

> *G. An assessment of privacy and civil rights and civil liberties requirements associated with the National Artificial Intelligence Research Resource and its research;*

Facial recognition technology has traditionally been developed by teams of primarily white and Asian men, and without representation from anyone of African descent or any Latino team members. And the data sets being used to train facial recognition AI are far from diverse enough. This lack of diversity has led to very real consequences of biased AI, from a man who was wrongfully arrested for a crime he did not commit to a young woman being improperly denied access to a skating rink earlier this year.[4]

---

[3] *See, e.g.*, *#StartupsEverywhere: Chasity Wright, Founder and CTO, Infiltron*, Engine (Nov. 11, 2020), https://www.engine.is/news/startupseverywhere-warner-robins-ga-infiltron.

[4] *See, e.g.*, Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y.T. (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; Randy Wimbley & David Komer, *Black Teen Kicked Out of Skating Rink After Facial Recognition Camera Misidentified Her*, Fox2 Detroit (July 14,

This substantial potential for bias permeates across sectors where AI is already being used, like the Transportation Security Administration and U.S. Customs and Border Protection are using facial recognition technology at airports.[5] The military is looking to use facial recognition for security at bases.[6] To avoid bias in these and every other aspect of our lives, the government (along with everyone else) needs to be using the best software that is inclusive of all backgrounds, and with checks and balances on when and how facial recognition can even be used.

Infiltron works with diverse teams, and that diversity will show in what we are building—technology that attends to accuracy and defends against bias. And Infiltron is focused on biometric accountability,[7] through our Biometric Legal Compliance and Governance Standard Protocol® and Biometric Technology Equality Standard®. Our software gathers and audits human biometric data, with an eye toward enhancing security, enforcing accountability, and mitigating risks (for example, legal and ethical risks).

The government must also prioritize diversity—in the NAIRR's leadership (as noted above),[8] as well as in the research teams it supports. But the problem, and the solution, run much deeper, to the data used to train AI systems. The NAIRR should prioritize providing multiple, unbiased data sets that ensure the broad array of all backgrounds are represented (for example, data sets that can look at hues of skin color). Startups and AI researchers need to be able to leverage those sorts of data sets when training AI systems.

As a customer and end-user of technology, the government should also expect its vendors to provide responsible technology that was developed through the use of good data. For the NAIRR's purposes, it could consider building in stipulations about how this government support should (and should not) be used. And the Task Force should maintain open and active lines of communication across the government—from policymakers to procurement—so that lessons learned through the resource about responsible development and deployment of AI can benefit others, and likewise so that the NAIRR's resources and best practices can be informed by other branches of government with relevant experience.

2021), https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her ; Dave Gershgorn, *Black Teen Barred from Skating Rink by Inaccurate Facial Recognition*, The Verge (July 15, 2021), https://www.theverge.com/2021/7/15/22578801/black-teen-skating-rink-inaccurate-facial-recognition.

[5] David Oliver, *Facial Recognition Scanners Are Already at Some U.S. Airports*, USA Today (Aug. 16, 2019), https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everything-you-need-know/1998749001/.

[6] Singh Bisht, *U.S. Army Calls for Facial Recognition Tech to Secure Bases*, The Defense Post (Apr. 6, 2021), https://www.thedefensepost.com/2021/04/06/us-army-facial-recognition-bases/.

[7] *Biometric Accountability*, Infiltron, https://infiltron.net/biometricaccountability/.

[8] *Supra* response to question I.C.

Response to Question 2. Which capabilities and services (see, for example, item D above) provided through the NAIRR should be prioritized?

AI trustworthiness assessments are critical, and should be included among the NAIRR's priorities. AI trustworthiness refers to evaluating AI systems against their stated solution, looking at things like "accuracy, explainability and interpretability, privacy, reliability, robustness, safety, and security (resilience) and mitigation of harmful bias."[9] For example, autonomous vehicles need to recognize stop signs even if they are marked with graffiti or obstructed by a tree branch. The car still needs to know that there is a stop sign there, and respond accordingly.

As the NAIRR Task Force considers what infrastructure the government will put in place, it should consider working towards better trustworthiness assessments. For example, the government can develop best practices or tools small companies can use—when they are just launching or getting started—to assess the trustworthiness of their AI solutions. Companies, including startups, need ways to test their AI, to make sure it is dependable and that it does not open up gaps for, e.g., hackers.

Response to Question 3. How can the NAIRR and its components reinforce principles of ethical and responsible research and development of AI, such as those concerning issues of racial and gender equity, fairness, bias, civil rights, transparency, and accountability?

The NAIRR can play a critical role promoting ethical, accountable, and trustworthy AI, and presents a unique opportunity to instill best practices that will last throughout product and company life cycles. As noted above, including diverse individuals in the development and governance of the NAIRR; ensuring multiple, unbiased datasets; and providing tools and best practices for trustworthiness can help promote these goals. [10]

Response to Question 6. Where do you see limitations in the ability of the NAIRR to democratize access to AI R&D? And how could these limitations be overcome?

Most innovative companies have (and will continue to have) some component of AI or leverage AI in their products. Ensuring startups access to the NAIRR would help more small companies compete and find success by lowering barriers to AI development. At the same time, with the proliferation of AI in business and as noted in above, the NAIRR can play a critical role in promoting best-practices for developing AI that is trustworthy and unbiased.[11] The NAIRR Task

[9] *Overview: Artificial Intelligence*, NIST, https://www.nist.gov/artificial-intelligence.
[10] *Supra* response to question 1.
[11] *Supra* responses to questions 1, 3.

Force should facilitate broad access for startups and other researchers, in order to achieve its aims of democratizing access and ethical AI development. To that end, it should also conduct proactive outreach to startups and members of the startup ecosystem, including with a special focus on historically underrepresented founders, to further the impact of the NAIRR.