Federal Register Notice 88 FR 7999, Federal Register : Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

The App Association (ACT)

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

March 3, 2023

National Science Foundation
Networking and Information Technology Research and Development
National Coordination Office
2415 Eisenhower Ave
Alexandria, Virginia 22314

RE: ***Comments of ACT | The App Association Regarding the Networking and Information Technology Research and Development National Coordination Office's 2023 Updates to the Federal Cybersecurity Research and Development Strategic Plan***

ACT | The App Association, hereby, submits comments in response to the Networking and Information Technology Research and Development National Coordination Office's (NITRD NCO) request for input on its 2023 update to the federal cybersecurity research and development strategic plan to guide and coordinate federally funded research in cybersecurity education, workforce development, and the development of consensus-based standards and best practices in cybersecurity. The App Association appreciates the opportunity to share our thoughts to aid in the formulation of a national strategy that addresses cyber training, education, digital awareness, and the cyber workforce.[1]

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology.[2] Enhancing an app ecosystem worth more than $1.7 trillion and responsible for 5.9 million American jobs, our members' innovations will continue to grow and power the rise of the internet of things (IoT).[3] The app economy creates employment opportunities for people in all parts of the country with a variety of skill sets.

Our dynamic, internet-enabled world carries a growing threat of cyber-attacks and American workers and students must be prepared to engage in the digital economy in a safe and secure way. All sectors of the U.S. economy increasingly depend on a workforce equipped with computer science skills; therefore, the growing scarcity of workers with a computer science background is placing America's global leadership in peril and undermining our country's

[1] National Science Foundation, *Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan*, available at https://www.federalregister.gov/documents/2023/02/07/2023-02578/request-for-information-on-the-2023-federal-cybersecurity-research-and-development-strategic-plan

[2] *See* http://actonline.org/about.

[3] ACT | The App Association, *State of the U.S. App Economy: 2020 (Seventh Edition),* available at https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf

national security. Per a study by the Center for Strategic and International Studies, the United States needs between 10,000 and 30,000 cybersecurity specialists to effectively address cybersecurity issues; however, there are only about 1,000 security specialists in the United States with the set of skills necessary to operate effectively in cyberspace. The App Association strongly urges the U.S. government to take steps to provide our current and future workforce with the necessary skillset to succeed in the jobs that will drive our economic development and protect our national security.

The App Association urges for the updated federal cybersecurity research and development strategic plan to align with the following:

- ***Supporting U.S. Leadership in Artificial Intelligence:*** Artificial intelligence (AI) is an evolving constellation of technologies that enable computers to simulate elements of human thinking, such as learning and reasoning. An encompassing term, AI entails a range of approaches and technologies, such as machine learning (ML), where algorithms use data, learn from it, and apply their newly-learned lessons to make informed decisions, and deep learning, where an algorithm based on the way neurons and synapses in the brain change as they are exposed to new inputs allows for independent or assisted decision-making. Already, AI-driven algorithmic decision tools and predictive analytics have substantial direct and indirect effects in consumer and enterprise context and show no signs of slowing in the future.

  Across use cases and sectors, AI has incredible potential to improve consumers' lives through faster and better-informed decision-making, enabled by cutting-edge distributed cloud computing. Even now, consumers are encountering AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition, all forms of what we consider "narrow" AI. These narrow applications of AI already provide great societal benefit. As AI systems, powered by streams of data and advanced algorithms, continue to improve services and generate new business models, the fundamental transformation of economies across the globe will only accelerate.

  Nonetheless, AI also has the potential to raise a variety of unique considerations for policymakers. ACT | The App Association encourages approaches to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers, consistent with consensus policy principles we have developed based on the consensus of our small business innovator community (appended to this comment letter).

- ***Advance Privacy Enhancing Technologies:*** The App Association encourages for the prioritization of privacy enhancing technologies (PETs), in alignment with the efforts of the Office of Science and Technology Policy (OSTP). PETS are an important tool for unlocking the full potential of the data economy and can help ensure that innovation in emerging technologies runs concurrently with a respect for basic human rights, promotes equity in data processing activities, and increases trust in the digital economy writ large. Consumers who rely on our members' products and services expect that our members will keep their valuable data safe and secure. The small business developer community the App Association represents practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, ensuring that the company's business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a marketdriven necessity. For this reason, we support the Administration’s goal of ensuring the United States leads the world in responsible data practices and technologies, including PETs, which are critical to our economic prosperity and national security, and to maintaining the core values behind America's scientific leadership, including openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

- ***Supporting Strong Encryption:*** The app economy depends on technical data protection methods and strong encryption techniques to keep users safe from harms like identity theft. However, some, including within the U.S. government, insist that “backdoors” be built into encryption for the purposes of government access. These policies would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a security and privacy standpoint, the viability of app developers’ products depends on the trust of end users. In alignment with leading policy and research from the National Institute of Standards and Technology, the App Association encourages the updated federal cybersecurity research and development strategic plan to prioritize advancing and supporting the use of advanced encryption techniques.

- ***Investing in (and Investigating) Quantum Computing:*** While advances in quantum computing offer the opportunity for incredible advances across a range of use cases, and should be prioritized and supported in the updated federal cybersecurity research and development strategic plan. At the same time, quantum computing presents the possibility of compromising encryption techniques widely relied upon across enterprise and consumer contexts.

- ***Developing the Cybersecurity Workforce:*** Generally, the App Association’s community notes misalignment in and between the public and private sectors regarding workforce categories, specialty areas, work roles, and skill sets. And in the cybersecurity context, the workforce must contend with constantly evolving threats. We support U.S. government efforts to provide building blocks for the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams in the National Institute of Standards and Technology’s (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity,[4] and urge NITRD NCO to support and align itself with this key initiative.

  Currently, cybersecurity professionals have access to a wide variety of valuable education programs to keep them up to date on the latest cybersecurity trends and certifications. Unfortunately, these programs are often prohibitively expensive, creating a barrier for small businesses and their employees. The App Association believes market effects should define the success of certification programs, and strongly discourages the development of a cybersecurity workforce that endorses particular third-party certification programs. Cybersecurity professionals, particularly those in small businesses, should have the flexibility to utilize certifications to build their expertise in any, and all, areas of data security, and updates to the strategy should support this concept.

  Beyond the growing need for cybersecurity professionals, we urge the strategy reflect that while universities are increasingly offering degrees in computer science and related fields, it is not currently known how well-ingrained cybersecurity is into such computer science curriculum. While we believe the U.S. government should support the universitylevel development of a U.S. cybersecurity workforce curriculum across classes (as opposed to standalone classes), cybersecurity education programs within public and private sectors will vary in type and effectiveness. There is currently no standard, scalable training, education, or awareness program for the cybersecurity discipline; this has resulted in industry groups offering their own solutions to this challenge. While more needs to be done, we applaud and appreciate the U.S. government's prioritization of cybersecurity education through grants and public-private partnerships.

We have witnessed firsthand that cybersecurity professionals must be well-versed in a wide range of technologies and potential risk vectors, including industry-specific skills such as supervisory control and data acquisition (SCADA) in the energy industry, or blockchain in the financial industry. We urge the U.S. government to help employers invest in the education and training of their current cybersecurity workforce and to utilize innovative programs, such as apprenticeships, to build the future workforce.

As IoT, cloud-based services, and cognitive computing play an increasingly vital role in our world, the demand for skilled cybersecurity professionals will steadily rise. While artificial intelligence and cognitive computing will greatly assist cybersecurity professionals in predicting and responding to cyber-based attacks, these technologies have their own vulnerabilities that will need to be addressed by security and data professionals.

The App Association appreciates the opportunity to weigh in on the 2023 federal cybersecurity research and development strategic plan on cyber training, education, workforce development, and best practices. We commit to working with all stakeholders to achieve a competitive and robust cybersecurity workforce in the United States.

Sincerely,

[redacted]

Brian Scarpelli
Global Senior Policy Counsel

Leanna Wade
Regulatory Policy Associate

ACT | The App Association
1401 K St NW (Suite 501)
Washington, District of Columbia 20005