SIA
SECURITY INDUSTRY ASSOCIATION

March 17, 2021

The Honorable Joseph R. Biden
President of the United States
1600 Pennsylvania Avenue, NW
Washington, D.C. 20500

The Honorable Kamala D. Harris
Vice President of the United States
1600 Pennsylvania Avenue, NW
Washington, D.C. 20500

Dear President Biden and Vice President Harris:

On behalf of the Security Industry Association (SIA), congratulations on your election as President and Vice President of the United States. We look forward to working with your administration and Congress to improve the security and livelihoods of Americans across our country.

SIA represents over 1,100 innovative companies that provide safety and security technology solutions essential to public safety and the protection of lives, property, information, and critical infrastructure. In the federal procurement sector, SIA members include companies that provide advanced security solutions to the U.S. Department of Homeland Security, the U.S. Department of Justice, the U.S. Department of Defense, the U.S. Department of Transportation, and their component agencies.

Our core mission is to serve as a catalyst for success within the security industry by promoting the effective and responsible use of technology by law enforcement, government personnel, and commercial entities. In fact, SIA maintains a strong commitment to ensuring our members uphold the highest standards of ethical conduct when deploying our technology, and this commitment is shown in SIA's Membership Code of Ethics.[1]

One issue that has become increasingly scrutinized is the use of biometrics in government and commercial applications – in particular, the use of facial recognition technology. SIA believes all technology products, including facial recognition, must only be used for purposes that are clearly defined, lawful, ethical, and non-discriminatory. When used appropriately, facial recognition has many proven benefits, such as aiding efforts to reunite victims of human trafficking with their loved ones, solving counterterrorism investigations in critical situations, cracking cold cases, facilitating safe travel, and detecting travelers using fraudulent documents to enter the United States.[2]

Like any other technology, such as cellular phones, information technology systems, and virtual meeting software, advancements in facial recognition technology are a direct result of consistent innovation and

[1] *See "SIA Membership Code of Ethics"*
https://www.securityindustry.org/about-sia/sia-membership-code-of-ethics/

[2] *See SIA Facial Recognition Success Stories Showcase Positive Use Cases of the Technology*
https://www.securityindustry.org/2020/07/16/facial-recognition-success-stories-showcase-positive-use-cases-of-the-technology/

research and development investments that ensure accuracy and reliability reach its maximum potential. Additionally, SIA members also have consistently sought to address concerns about bias and potential misuse of facial recognition technology by: (1) improving its algorithmic accuracy across all demographics; (2) encouraging law enforcement and government users to transparently publish privacy assessments; and (3) promoting the development and implementation of organizational policy that forbids the use of facial recognition in a discriminatory manner. While these measures are critical, it is important to note that the National Institute of Standards and Technology (NIST) – the agency which evaluates the accuracy of facial recognition algorithms through its facial recognition vendor test (FRVT) – confirmed in its most recent report on demographic effects that high-performing algorithms exhibited "undetectable" differences in accuracy measures across race and other demographic factors.[3] [4]

Instead of focusing on legislation and policies that would provide a constructive framework for how facial recognition can be used responsibly, some critics have called for a ban or moratorium on the use of this technology. SIA strongly opposes this approach, which would severely limit the ability of law enforcement and government personnel to perform duties critical to public safety and security. A lack of U.S. leadership in modeling responsible technology use also would cede ground to our adversaries who, unlike the U.S., allow use of facial recognition technology in unconstrained ways, which could establish a standard of practice abroad that impacts human rights, exacerbates pervasive mass-surveillance practices, and enables our adversaries to outperform the U.S. in future technology innovation.

SIA requests that Congress and the administration consider three recommendations to support improvements in facial recognition technology while promoting its responsible use and America's leadership role.

1. Expanded Research Activities and Funding for the NIST Image Analysis Unit

The NIST FRVT program is known globally as the gold standard for scientifically testing the quality and accuracy of facial recognition technology. FRVT and other activities of the NIST Image Analysis Unit within the Information Technology Laboratory provide critical resources for law enforcement, government, and commercial entities to assess the quality of their facial recognition technologies. However, as NIST and Congress have pointed out in past congressional hearings, these programs lack the full resources needed to carry out expanded testing activities NIST has identified to more thoroughly and regularly evaluate performance of the technology across demographic variables, test the full range of available algorithms, coordinate with federal agencies that deploy facial recognition in the field, and assess identification processes incorporating both facial recognition technology and trained human review.

We urge the administration to include in its budget request for FY22, an increase under NIST's Scientific and Technical Research and Services program specifically for expanding and speeding up the timeline for NIST research and evaluation of facial recognition technologies.

[3] *See Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, 8,* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[4] *See What NIST Data Shows About Facial Recognition and Demographics* https://www.securityindustry.org/2020/02/14/what-nist-data-shows-about-facial-recognition-and-demographics/

2. Direct Additional NSF Funding to HBCUs, HSIs, and Other Minority Institutions

Through FY21 appropriations measures, Congress directed the National Science Foundation (NSF) to leverage artificial intelligence (AI) related grant opportunities and interdisciplinary research initiatives by focusing its outreach and engagement with community colleges, Historically Black Colleges and Universities (HBCU), Hispanic Serving Institutions (HSI), and Minority Serving Institutions (MSI).

SIA supported this language, and in the context of facial recognition and other technologies developed using AI and machine learning, there needs to be greater minority representation in research and development activities. There is an opportunity for Congress and the administration to instruct NSF to work with community colleges, HBCUs, HSIs, and MSIs to develop academic curriculum and workforce development programs in the biometrics field. This approach would help these students receive the necessary skills to succeed in biometrics related career fields. Moreover, interdisciplinary research focused on facial recognition algorithmic development will provide students with first-hand knowledge about the challenges and opportunities presented by these advanced technologies, including issues surrounding performance differentials and bias mitigation, and help create a diverse talent pipeline of individuals that are well positioned to address solutions.

3. Promote Policies That Strengthen Transparency and Build Public Trust Regarding Use of Facial Recognition Technology

We encourage the administration to review *SIA's Principles for the Responsible and Effective Use of Facial Recognition Technology,* which include policy recommendations for promoting the ethical, transparent, and defined use of facial recognition technology by the government, law enforcement, and the commercial sector.[5] In particular, we outline measures that could increase accountability, accuracy and data security for public sector applications, and ensure law enforcement uses only for legitimate and constitutional purposes. We urge that continued development of rules regarding use of this technology take into account vast differences between the purpose and impact of various public and private sector applications, where the specific privacy considerations and significance of the identification process depend on the specific application.

Additionally, the principles align strongly with U.S. Government Accountability Office (GAO) recommendations for addressing DHS and commercial use of facial recognition:

- For U.S. Customs and Border Protection (CBP) and Transportation Security Administration (TSA) use, GAO lists five recommendations for DHS that address complete and conspicuous privacy notices for travelers, audit requirements for privacy compliance, performance thresholds, and more defined policies for traveler photo capture.[6]

[5] *See "SIA Policy Principles for the Responsible and Effective Use of Facial Recognition Technology"* https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

[6] *See Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, https://www.gao.gov/assets/710/709107.pdf

- In the commercial sector, GAO reiterated its September 2013 recommendation that any forthcoming legislation should leverage "…a consumer privacy framework to reflect changes in [facial recognition] technology and the marketplace."[7] For many such applications the benefits already rely on voluntary agreements from individuals and offer to those individuals increased security, safety, and convenience.

SIA looks forward to working with the administration and Congress to improve facial recognition technology and ensure its responsible use by government and commercial end-users. Thank you for considering SIA's views and recommendations on this important issue.

Sincerely,

Don Erickson

Don Erickson, CEO
Security Industry Association

CC: National Security Council
Office of Public Engagement
Office of Science and Technology Policy

[7] *See Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses*, July 2020. https://www.gao.gov/assets/710/708045.pdf; *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, September 2013. https://www.gao.gov/assets/660/658151.pdf