July 13, 2021

The Honorable Sheila Jackson Lee
Chairwoman
House Committee on Judiciary, Subcommittee
on Crime, Terrorism, and Homeland Security
6340 Neil House Office Building
Washington, DC 20515

The Honorable Andy Biggs
Ranking Member
House Committee on Oversight and Reform
on Crime, Terrorism, and Homeland Security
6340 Neil House Office Building
Washington, DC 20515

Dear Chairwoman Jackson Lee and Ranking Member Biggs:

On behalf of the Security Industry Association (SIA), thank you for holding today's hearing focused on law enforcement's use of facial recognition technology. 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. 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, and their component agencies.

SIA believes all technology products, including facial recognition, must only be used for purposes that are clearly defined, lawful, ethical, and non-discriminatory. SIA has taken steps to support related polices by: 1) developing and publishing policy principles that will help ensure facial recognition is used in a responsible and effective manner; 2) providing specific policy recommendations to the Biden Administration and Congress that address concerns about facial recognition technology while maintaining U.S. leadership in future development; and 3) providing information regarding the benefits of many technology applications, including success stories from over a decade of use in U.S. law enforcement investigations, such as a how facial recognition technology was used to help rescue a child sex trafficking victim in California, identify a serial armed robber in Indiana, help verify the identity of a man in Pennsylvania accused of sexually assaulting a 15 year-old girl, and help identify an alleged rapist in New York City, to name just a few of many thousands.

Responsible implementation and use of facial recognition technology should include appropriate transparency and accountability measures, stakeholder education, and addressing privacy considerations and civil liberties protections. The June 2021 GAO report entitled, *Facial Recognition: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* provides an in-depth review of how Federal agencies that employ law enforcement officers use facial recognition technology to assist in criminal investigations and recommends implementing additional internal mechanisms and policies that ensure Federal personnel track what non-federal systems – e.g., state, local, tribal, or territorial entities – are used by their employees. Agencies should have full visibility into the technologies relied upon for criminal investigations and have measures in place to ensure personnel are using facial recognition systems for defined and authorized purposes. Furthermore, GAO recommends that Federal agencies assess certain risks of using these systems, including privacy and accuracy-related risks, so agencies are better positioned to mitigate potential risks to themselves and the public. SIA strongly supports measures

that increase transparency across the Federal government with respect to use of facial recognition technology and continue to build public trust that it is being used effectively and appropriately.

At the request from members of the House Science, Space & Technology committee, GAO released a relevant technology assessment in July 2021 entitled, *Forensic Technology: Algorithms Strengthen Forensic Analysis, but Several Factors Can Affect Outcomes*. GAO provided law enforcement agencies with another series of policy recommendations to improve its use of forensic technologies and algorithms – including facial recognition algorithms. After conducting extensive research, GAO did not recommend a ban or moratorium on the use of facial recognition algorithms. Rather, GAO found that "facial recognition algorithms help analysts extract digital details from an image and compare them to images in a database. These algorithms can search large databases faster and can be more accurate than analysts." Within the assessment, GAO acknowledged the value of the technology and the opportunity to address various challenges related to law enforcement's use of facial recognition algorithms by recommending robust policy options to: 1) increase personnel training that could reduce risks created by human error, address cognitive biases and improve objectivity in analyses, and provide analyst certification processes; 2) apply flexible, consensus-driven standards for testing and performance of facial recognition algorithms; and 3) improve public access to test data that is constructed in a legible format that increases transparency and builds public trust among communities. SIA recognizes that additional work and innovation is required in order to fully develop related policy proposals, but our industry is encouraged by GAO's constructive recommendations.

SIA and our members stand ready to contribute to a constructive dialogue surrounding facial recognition technology. Please let us know if there is any way we can assist you as you continue to examine these issues.

Sincerely,

Don Erickson

Don Erickson
CEO – Security Industry Association

Cc: Members of the House Judiciary Committee

For more information, please contact Joe Hoellerer, SIA Senior Manager of Government Relations, at jhoellerer@securityindusry.org