

December 21, 2020

The Honorable Chad Wolf
Acting Secretary
U.S. Department of Homeland Security
2707 Martin L. King Avenue, SE
Washington, DC 20528

Re: Concerns Regarding Department of Homeland Security's Proposed Rule Entitled "Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States" via Docket Number USCBP-2020-0062.

Dear Acting Secretary Wolf:

On behalf of the physician and medical student members of the American Medical Association (AMA), I welcome the opportunity to provide comment on the U.S. Department of Homeland Security's (DHS or the Department) proposed rule concerning the Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (USCIS). DHS is proposing to implement a national biometric entry and exit program, focusing on the use of facial recognition technology, which also would permit the collection of biometric information beyond photographic images. We recognize that policymakers often must balance issues of national security—including implementation of new security technology—with intrusions on individual privacy and liberty. However, any entity seeking access to an individual's health information (including biometric information) must pass the stringent test of showing why its professed need should override the individual's most basic right in keeping his or her own information private. DHS has failed to make such a justification, and in fact is proposing to legitimize a tool shown by multiple studies to be inaccurate due to bias. **The AMA urges DHS to withdraw its proposal until the data of participants can be adequately protected and the accuracy of facial recognition technology has increased such that it does not contain racial, age, and gender biases.** We address a few of the more pertinent privacy, ethical, and social equity-related issues below.

DHS must be specific about its intended use of biometric information and avoid creating blanket permissions to collect biometrics.

In addition to DHS' proposal that aliens arriving and departing the U.S. be photographed for identification purposes, DHS is proposing to require that most aliens entering and departing the U.S. "provide other biometrics" and "other such evidence as may be requested." This is an overly broad and ambiguous proposal, particularly in light of DHS' note that "a biometric refers to a form of identification based on anatomical, physiological, and behavioral characteristics or other physical attributes unique to a person that can be collected, stored, and used to verify the identity of a person, e.g., fingerprints, photographs, iris, DNA, and voice print."¹ We are opposed to this attempt to create a vague blanket permission for DHS to collect biometric information. Absent stringent guidelines and explicit limitations

¹ 85 Fed. Reg. 74162 (Nov. 19, 2020) at 74163, footnote 1; <https://www.federalregister.gov/d/2020-24707/p-85>.

surrounding the use of biometrics by DHS in the proposed rule, we have serious concerns that the agency could inappropriately expand their biometric protocols without public input and consideration of unintended consequences.²

Facial recognition technology has serious racial, gender, and age biases that lead to considerably decreased accuracy for this technology and should not be used by DHS until these issues are resolved.

In a significant change from current policy, which restricts DHS to voluntary collection of biometrics from certain immigrants upon departure under pilot programs at certain airports, seaports, and land ports, DHS now proposes to collect biometrics from “aliens” entering or departing from airports, land ports, seaports, or any other authorized point of departure. Specifically, all aliens may be required to be photographed upon entry and departure from the U.S. regardless of age or visa classification for the purpose of utilizing facial recognition technology to confirm an alien’s identity.³

Although DHS has been working to implement facial recognition technology as a primary identification tool at all points of entry and exit within the United States, there remain significant concerns regarding the accuracy and capabilities of such technology. Studies have found that accuracy of facial recognition technology is linked to physical factors including pose, illumination or expression of a face, cosmetics, glasses, hair, or other easily changeable characteristics that may cover parts of a face, general image quality, inherent facial characteristics, particularly skin reflectance or underlying facial structure, and aging over time.⁴ Moreover, DHS acknowledges in its proposal that “[c]ertain human factors, such as traveler attire and attentiveness, did impact technology effectiveness.”⁵ A recent study from the National Institute of Standards and Technology (NIST) found that the majority of facial recognition algorithms in the industry possess biases that span race, gender, and age. “While it is usually incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied,” said Patrick Grother, a NIST computer scientist and the report’s primary author. “While we do not explore what might cause these differentials, this data will be valuable to policymakers, developers and end users in thinking about the limitations and appropriate use of these algorithms.”⁶

The NIST study evaluated 189 software algorithms from 99 developers—a majority of the industry. It focuses on how well each individual algorithm performs one of two different tasks that are among face recognition’s most common applications. The first task, confirming a photo matches a different photo of the same person in a database, is known as “one-to-one” matching and is commonly used for verification work, such as unlocking a smartphone or

² <https://searchlf.ama-assn.org/letter/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2020-10-13-Letter-to-Wolf-re-DNA-Biometrics-IFR-v2.pdf>.

³ <https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states>.

⁴ <https://www.gao.gov/assets/710/708045.pdf>.

⁵ <https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states>.

⁶ <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

checking a passport. The second, determining whether the person in the photo has any match in a database, is known as “one-to-many” matching and can be used for identification of a person of interest.⁷

In order to evaluate whether each algorithm can sufficiently complete the “one-to-one” and/or “one-to-many” matching protocols, researchers collected data on the two types of potential software errors: false positives and false negatives. A false positive means that the software wrongly recognized photos of two different individuals as the same person, while a false negative means the software failed to match two photos that show the same person. As such, there are countless factors that can, and do, negatively impact the accuracy of “one-to-one” and “one-to-many” matching.

Any federal policy suggesting the use of facial recognition technology must demonstrate that it is accurate and unbiased. Race and ethnicity are fundamental demographics to consider when determining the quality and accuracy of facial recognition technology. This is especially relevant considering that the algorithms designed to pilot these facial recognition technologies are not objective in nature but fluctuate widely depending on the demographic of the creator themselves. As an illustration of these algorithmic biases NIST’s test revealed that facial recognition algorithms that were developed in China showed low false positive rates on East Asian faces.⁸ On the other hand, facial recognition algorithms that were developed in the U.S. and Western Europe were 10 to 100 times more likely to inaccurately identify a photograph of a black or East Asian face, compared with a white one.⁹ With such a wide variation across algorithm development, this produces significant discrepancies in the false non-match rate which has been found to be between 0.1 percent and 10 percent.¹⁰ This variation is unacceptable in a technology policy that will impact individuals from all races and ethnicities.

Additionally, a July 2020 Government Accountability Office (GAO) report analyzing DHS’ pilot facial recognition program noted that DHS’ facial recognition technology is still struggling with algorithmic biases.¹¹ Moreover, GAO officials stated that DHS’ analysis of its pilot facial recognition programs is limited due to lack of data on age, gender, and ethnicity for travelers entering and exiting the country.¹² Therefore, acknowledging the significant impact that race and ethnicity demographics have on matching rates produced by facial recognition technology, the efforts of DHS to accurately identify individuals entering and exiting the U.S. is severely limited without the collection and evaluation of this data on race and ethnicity in their algorithms and thus, should not be implemented until this obvious and extreme bias is remedied.

These biases are so persistent within facial recognition technology that in addition to NIST, other recent academic studies and independent evaluations have reported performance trends similar to what NIST found among demographic groups noting that Asian, Native groups, and African American people were misidentified as much as 100 times more than white men.¹³ For instance, four studies on verification

⁷ <https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states>.

⁸ <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

⁹ *Id.*

¹⁰ <https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/>.

¹¹ <https://www.gao.gov/assets/710/708045.pdf>.

¹² *Id.*

¹³ <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

algorithms noted that performance was lowest on women, black people, and very young or very old people in comparison to performance on middle-age white men.¹⁴ To contextualize this, “[i]n verification algorithms, false positive rates for white males and black females varied by factors of 10 to more than 100, meaning the lowest-performing algorithm could be over 100 times more accurate on white male faces than on black female faces. Additionally, for verification and identification vendor tests, false positives were higher for women than men.”¹⁵ These differences are very likely to result in more frequent misidentification for the individuals that would be forced to participate in the program.

Moreover, additional studies found constant biases in favor of white men with error rates never worse than 0.8 percent when determining the gender of light-skinned men. However, women in the studies were more often inaccurately identified with a correlation between darker skin tone and a higher error rate.¹⁶ For medium skinned women the error rates were between 20.8 and 34.7 percent. But, for the darkest-skinned women in the data set the error rates increased to between 46.5 and 46.8 percent.¹⁷ For those women, the technology was doing little more than guessing their gender at random. The U.S. companies that owned this facial recognition algorithm claimed an accuracy rate of more than 97 percent. However, the data sets used to assess this performance were more than 77 percent male and more than 83 percent white.¹⁸ As such, this technology not only had biased results, but the proprietors of these technologies claimed a greater accuracy than was actually warranted based on the limited data set on which the algorithm was trained. These studies underscore our concerns with the federal government using a technology to identify individuals when such technology is unable to distinguish gender and race accurately and consistently.

DHS is proposing to collect biometric data from all immigrants regardless of their age. DHS asserts that this expanded collection of biometric data will enable the agency to associate the immigration records created for children to their future adult records. DHS contends that this expanded collection will aid in combatting children trafficking, and the ability to confirm the absence of criminal history or associations with terrorist or other criminal organizations.¹⁹ Current regulations that exempt the biometric collection of individuals under 14 and over 79 are based on technological limitations and traditional law enforcement policies, such as not running criminal history background checks on children.²⁰ However, the Department asserts that the current regulations are not applicable to its facial recognition-based biometric entry-exit program, since it believes new technology is more accurate. Such claims are inaccurate on their face: **evidence from the NIST study shows that the natural aging process changes an individual’s appearance over decades, ultimately undermining automated facial recognition:**

Age itself is a demographic factor as accuracy in the elderly and the young differ for face recognition (usually) and also for fingerprint authentication. This applies even without significant time lapse between two photographs. We found elevated false positives in the elderly and in children; the effects were larger in the oldest

¹⁴ <https://www.gao.gov/assets/710/708045.pdf>.

¹⁵ *Id.*

¹⁶ <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212?s=09>.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ <https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states>.

²⁰ <https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states#p-263>.

and youngest, and smallest in middle-aged adults ageing is highly influential on face recognition false negatives. The effects are consistent across country-of-birth, datasets and algorithms but vary in magnitude.²¹

The swiftly changing facial features associated with aging, a physiological process that occurs in all children, increases the likelihood of both false positive and false negative identifications for this demographic. These errors will not only have immediate impacts on the individual when trying to enter the U.S. but could also harm these individuals and their families in the future. For example, one of the goals set out by DHS with implementation of this technology is to prevent human trafficking across the nation's border. However, due to the risks of false matching, a child may be identified as missing or trafficked, even when this is not true, and their family could potentially be separated or falsely detained. Therefore, prior to implementing this mandatory facial recognition protocol across all age groups, DHS should further research ways to mitigate demographic differentials with respect to false positives and false negatives, especially in children and the elderly.

Across a multitude of studies, it has been shown that white middle-aged males are the demographic that is consistently correctly identified. The remainder of the population is consistently misidentified with varying rates of false positives and false negatives. With mounting concerns surrounding the accuracy of facial recognition technology, and the presence of bias within the technology, there has been a growing movement to curb this technology's use. From companies refusing to sell their technology to local law enforcement,²² to local governments banning its use,²³ to Congress calling on the incoming Biden Administration to impose stricter regulations on facial recognition technology,²⁴ a wide range of stakeholders recognize the "clear bias based on ethnic, racial, gender, and other human characteristics," which injure the rights of individuals in specific demographic groups.²⁵ Given the intended use of this technology, these biases could have dire consequence for individuals, including false accusations of terrorism, using false travel documents, or committing visa fraud. Since most immigrants to the U.S. are not middle-aged, white men, the use of this technology in this setting is irresponsible and unjust and will only serve to compound and embed bias into our immigration system.²⁶

The use of facial recognition technology, and other biometric collection methods, requires robust privacy protections which DHS currently does not have.

The AMA's approach to privacy is governed by our *Code of Medical Ethics* and long-standing policies adopted by our policymaking body, the House of Delegates, which support strong personal privacy protections. AMA policy and ethical opinions on privacy and confidentiality provide that an individual's privacy should be honored unless waived by the person in a meaningful way, is de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of privacy or breaches of confidentiality. When breaches of confidentiality are compelled by concerns for public health and safety, these breaches must be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest entities and

²¹ <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

²² <https://thehill.com/policy/technology/503077-facial-recognition-tools-under-fresh-scrutiny-amid-police-protests>.

²³ <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>.

²⁴ <https://www.rollcall.com/2020/12/08/advocates-to-press-biden-congress-on-facial-recognition-curbs/>.

²⁵ <https://www.nature.com/articles/d41586-020-03186-4>.

²⁶ <https://www.forbes.com/sites/thomasbrewster/2020/06/24/a-wrongful-arrest-of-a-black-man-provides-more-proof-facial-recognition-is-racist/?sh=2584c6da5deb>.

individuals as possible to achieve the necessary end. However, the proposed rule does not fall within narrowly defined exception.

DHS' proposal fails to provide individuals with choice over whether their personal information will be used to develop and/or train machines or algorithms.

Facial recognition technologies perform three basic functions: detection, which is the recognition that there is a face in an image; verification, the confirmation of the identity associated with the face; and identification, the matching of an image of an unknown face to a gallery of known people.²⁷ For facial recognition technology to function, these systems rely on machine learning, a component of artificial intelligence in which the algorithm uses training data to identify patterns and predict an answer to a question, such as “what parts of this face are important when figuring out who this person is?”²⁸

For this specific program, Customs and Border Patrol (CBP) has developed a matching service for all biometric entry and exit operations that use facial recognition, regardless of the method of entry or exit. For all biometric matching deployments, the traveler verification system (TVS) relies on biometric templates generated from pre-existing photographs that CBP already maintains, known as a “gallery.” These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters. CBP builds “galleries” of photographs based on where and when a traveler will enter or exit. If CBP does not have access to the advance passenger information system (APIS) manifest information, such as for pedestrians or privately owned vehicles at land ports of entry, CBP will build galleries using photographs of “frequent” crossers for that specific point of entry that then become part of a localized photographic gallery. CBP’s TVS facial matching service then generates a biometric template for each gallery photograph that is stored in the TVS cloud and used to match travelers when they arrive or depart.²⁹ These images are then sent to a VFS database, which stores the Lane Security Controller facial images packages for analysis and processing.³⁰ CBP’s network then performs a post-analysis evaluation of facial images for photo quality and biometric matching accuracy.

Through this evaluation, CBP refines its approach to biometric matching. As such, CBP has been and plans to continue to take the images of individuals, regardless of their citizenship status, and use this information to track individuals and to train their machines to recognize faces. The AMA strongly opposes this approach. Our Privacy Principles state that individuals should have the right to know whether their data will be used to develop and/or train machines or algorithms and that the opportunity to participate in data collection for these purposes must be on an opt-in basis.³¹ Since this program is mandatory for immigrants and is an opt-out program for U.S. citizens, the proposed program violates privacy principles and must be altered in order to ensure that individuals are fully informed about, and given choice over, how their personal biometric data is used.

²⁷ <https://www.gao.gov/assets/710/708045.pdf>.

²⁸ *Id.*

²⁹ <https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states>.

³⁰ VFS Global is the world’s largest visa outsourcing and technology service specialist for governments and their diplomatic mission worldwide. See, <https://www.vfsglobal.com/en/governments/index.html>.

³¹ <https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf>.

DHS has failed to consistently provide the appropriate information for U.S. citizens to opt-out of the facial recognition entry-exit program.

DHS affirms that the proposed changes to expand biometric collection at U.S. ports of entry and exit would continue to require U.S. citizens to voluntarily opt-out if they do not want to participate. The ability for U.S. citizens to opt-out is widely supported in concept, as noted by the Federal Trade Commissions' Fair Information Practice Principles (FIPPs) which asserts that individuals should be able to consent to the use of their personally identifiable information to the extent possible. However, DHS has had persistent issues communicating this protocol from the beginning of its facial recognition pilot programs despite multiple GAO audits. As recently as September 2020, the GAO recorded gross violations of the FIPPs by DHS, including a lack of publicly available information on opting out of the pilot program's facial recognition identity verification, absent or concealed CBP facial recognition signs, and outdated information on the CBP webpage.³² The report also noted that when travelers would request to opt out of facial recognition identity verification, CBP notices provided limited information on the required process. Moreover, when individuals inquired about the process to opt-out, they were told by CBP officers and airline agents that opting out would lead to additional security scrutiny, increased wait times, and could be grounds to deny boarding.

The current privacy policies that govern DHS' actions, require that U.S. citizens be provided the ability to opt-out of the agency's biometric entry and exit programs. However, DHS has clearly neglected its duty to ensure that individuals have a clear understanding of their privacy rights, and information on how to opt-out of this facial recognition program, as noted by the GAO:

CBP has not ensured that it consistently provides travelers with complete and accurate information for its Biometric Entry-Exit Program nor has it ensured that notices are provided at all locations where facial recognition technology is used. Until CBP ensures that privacy notices contain complete and accurate information and that these notices are posted and visible for traveler review, CBP does not have assurance that the privacy protection principles designed to protect the personally identifiable information of the public are fully incorporated into its Biometric Entry-Exit Program. Nonetheless, including additional information about how to opt out on CBP's signs and other notices, as appropriate, would better ensure that travelers are aware of their rights and can make informed decisions about consenting to facial recognition identity verification. CBP has not consistently provided travelers with information about the locations where facial recognition is used, and CBP's privacy signage—which is intended to inform the traveling public of the use of facial recognition.³³

U.S citizens must be accurately and purposefully informed of their rights surrounding privacy and security. Despite assertions by DHS that photos taken by the facial recognition program will be deleted following 12 hours for U.S. citizens and up to 14 days for non-citizen travelers, in the pilot program CBP has been retaining sensitive, biographic entry and exit records for 15 years for U.S. citizens and 75 years for non-immigrant aliens.³⁴ Since CBP has not been removing U.S. citizen and non-citizen travelers records within the shortened timeframe, it is very unlikely that CBP will delete this information within 14

³²<https://www.gao.gov/assets/710/709107.pdf>.

³³ *Id.*

³⁴ *Id.*

days if the program is expanded and made permanent. As biometric surveillance technology continues to evolve, insufficient regulations could enable undetectable, persistent, and suspicionless surveillance on an unprecedented scale. This would permit the government to pervasively track people's movements and associations in ways that threaten privacy and due process rights. To ensure transparency, DHS must hold its programs to the highest standard of privacy protection, including those represented by the FIPPs, to prevent this technology from undermining fundamental constitutional values.³⁵

Until DHS and CBP are able to meet the goals set out by the GAO in its September 2020 report, which include ensuring that the Biometric Entry-Exit Program's privacy notices contain complete and current information, making known all of the locations where facial recognition is used, informing U.S. citizens on how travelers can request to opt out, ensuring that the privacy signage is consistently available at all locations where CBP is using facial recognition, and providing up to date information in all of CBP's communications, DHS should not proceed with its Facial Recognition Biometrics program.

DHS has failed to adequately protect personal biometrics data and sufficiently oversee its contracted partners, which has led to multiple serious data breaches thus demonstrating that DHS is unprepared to expand and permanently establish a nationwide entry-exit program.

DHS considers biometric information such as facial images to be sensitive personally identifiable information (SPII). The Department classifies certain forms of information as SPII because if lost, compromised, or disclosed without authorization, it could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.³⁶ As such, this data must be zealously protected.

This necessity to protect facial images is especially important since, the DHS Office of Biometric Identity Management maintains the Automated Biometric Identification System (ABIS), which contains the biometric data repository of more than 250 million people and can process more than 300,000 biometric transactions per day.³⁷ The ABIS "is the largest biometric repository in the Federal Government, and DHS shares this repository with the Department of Justice and the Department of Defense."³⁸

With multiple government contractors and millions of individuals' SPII involved, the AMA is highly concerned that DHS does not have the safeguards or capability to effectively manage the responsibilities surrounding the entirety of the collection, processing, and storage of facial recognition technology. Despite a multitude of audits by the GAO, CBP continues to fail to appropriately safeguard biometric technologies, including facial recognition software, and has repeatedly been found deficient by the GAO in ensuring appropriate security measure for data privacy. For example, shortly before the release of this proposed rule, the GAO published an audit highlighting critical concerns related to DHS' current use of biometrics. This audit found that facial recognition technology used by DHS and CBP to identify foreign nationals at various ports of entry had significant issues related to DHS' conduct and maintenance of privacy standards.³⁹

³⁵ <https://www.aclu.org/press-releases/aclu-challenges-fbi-face-recognition-secrecy>.

³⁶ <https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states>.

³⁷ <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf>.

³⁸ *Id.*

³⁹ <https://www.gao.gov/assets/710/709107.pdf>.

Accordingly, there have been multiple large-scale breaches of individuals SPII due to DHS' negligence. In early 2019, DHS experienced a data breach in which 2 million U.S. disaster survivors had their biometric information leaked.⁴⁰ Unfortunately, later in 2019, DHS experienced another major biometrics breach when Perceptics, LLC, a DHS subcontractor, was exposed to a cyber-attack that compromised approximately 184,000 traveler images from CBP's facial recognition pilot, at least 19 of which were posted to the dark web.⁴¹ Due to DHS' lax security practices, Perceptics, LLC, transferred copies of CBP's biometric data to its own company network, without CBP's knowledge, and was hacked.⁴² Prior to this data breach, CBP had not conducted any security or privacy audits of its contractors.⁴³ As such, the GAO found that CBP's information security practices during the pilot were inadequate to prevent the subcontractor taking possession of sensitive CBP-owned data.⁴⁴ Moreover, CBP inadequately remedied the breach by temporarily suspending Perceptics, LLC, from participation in future Government contracts in June of 2019 only to lift the suspension in September of 2019.⁴⁵

As stated in the proposed rule, DHS requires its commercial partners, such as airlines, to follow CBP's privacy and business requirements and can audit partners to assess compliance. However, as of May 2020, CBP had only audited one of its more than 20 airline partners despite its recent large scale data breach.⁴⁶ Moreover, as of September 2020, CBP did not have a plan to ensure that all of its partners were audited. According to the GAO, "[u]ntil CBP develops and implements an audit plan, it cannot ensure that traveler information is appropriately safeguarded."⁴⁷ This finding is especially disconcerting because if this proposed rule is implemented with the vulnerabilities that currently exist, and the entry/exit program continues to grow and encompass airports, seaports, and land ports, the security risks associated with this program will increase exponentially.

Notably, within the proposed rule, some partnership agreements with airlines or airports require the airline or airport staff, rather than CBP, to perform the TVS biometric collection. "Based on agreements with CBP, these stakeholders deploy their own camera operators and camera technology to operate TVS for identity verification."⁴⁸ As such, the equipment, cameras, and personnel are not guaranteed to be owned or employed by the government. Based off CBP's previous security breaches, and lack of supervision in the pilot program, DHS is providing highly sensitive SPII to a multitude of different contractors without adequate oversight, therefore compromising the privacy of millions of individuals. Additionally, allowing companies outside of the government to have access to, and own the hardware and software that execute the facial recognition searches, provides ample opportunity for malicious hacks or unethical use of this information. This limited privacy and security protection infrastructure demonstrates that DHS has insufficient safeguards in place to prevent sensitive materials from being exploited for malicious purposes. As such, we ask that DHS withdraw this proposed rule until it has reconciled these privacy and security concerns.

⁴⁰ <https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/>.

⁴¹ <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf>.

⁴² *Id.*

⁴³ <https://www.gao.gov/assets/710/709107.pdf>.

⁴⁴ <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf>.

⁴⁵ *Id.*

⁴⁶ <https://www.gao.gov/assets/710/709107.pdf>.

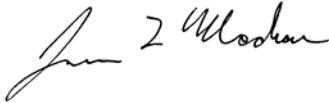
⁴⁷ *Id.*

⁴⁸ *Id.*

The Honorable Chad Wolf
December 21, 2020
Page 10

We appreciate the opportunity to comment and urge the Administration to prioritize the proper and accurate use of biometric data by withdrawing the proposed rule until the bias, privacy, and security concerns enumerated above can be remedied. We welcome the opportunity to share our views further. If you have any questions, please contact Margaret Garikes, Vice President for Federal Affairs, by calling 202-789-7409 or emailing margaret.garikes@ama-assn.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim L. Madara". The signature is written in a cursive, flowing style.

James L. Madara, MD