December 21, 2020

Michael Hardin, Director
Entry/Exit Policy and Planning
Office of Field Operations
U.S. Customs and Border Protection

Submitted via http://www.regulations.gov

Re: Department of Homeland Security, U.S. Customs and Border Protection, Notice of Proposed Rulemaking, Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States (Docket No. USCBP-2020-0062, RIN 1651-AB12)

Dear Mr. Hardin,

The American Immigration Council (Council) submits the following comments in opposition to the above-referenced Department of Homeland Security ("DHS") and U.S. Customs and Border Protection ("CBP") Notice of Proposed Rulemaking, *Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States* (USCBP Docket No. USCBP-2020-0062, RIN 1651-AB12) (hereinafter "Proposed Rule").

The Council is a non-profit organization established to increase public understanding of immigration law and policy, advocate for just and fair administration of our immigration laws, protect the legal rights of noncitizens, and educate the public about the enduring contributions of America's immigrants. The Council litigates in the federal courts to protect the statutory, regulatory, and Constitutional rights of noncitizens, advocates on behalf of noncitizens before Congress, and has a direct interest in ensuring that those seeking protection in the United States have a meaningful opportunity to do so.

I. The Council strongly opposes the Proposed Rule

Through this Proposed Rule, CBP proposes to require all noncitizens—including lawful permanent residents—to submit to the collection of facial images for duplicative identity verification through the expansive use of unproven facial recognition technology. Importantly, U.S. citizens will also be subjected to the same image collection unless they affirmatively opt-out at the time of their travel. DHS has failed to prove that the rule is truly necessary or justified. As drafted, the Proposed Rule will lead to sweeping and ongoing violations of the Privacy Act. Moreover, the Proposed Rule was promulgated under the purported authority delegated by the current Acting Secretary of Homeland Security who was improperly appointed to his role and therefore lacks the authority to both promulgate such rules on his own and to delegate such authority to others. The Council strongly opposes the Proposed Rule due to its considerable impact

on the privacy of both U.S. citizens and noncitizens attempting to enter and exit the United States. The Proposed Rule must be withdrawn.

II. DHS has failed to prove that the changes in the Proposed Rule are necessary or justified

CBP attempts to justify the dramatic expansion of biometrics collection and use of facial recognition technology by repeatedly citing concerns of fraud, largely relying on the possible use of valid travel documents by third party imposters, in addition to a stated need to identify visa overstays.[1] While national security and the integrity of the U.S. immigration system are areas of great concern, CBP has failed to prove that the changes it proposes would meaningfully improve upon the efficacy of the current systems and procedures already in place, or that the mass collection of facial recognition data is the least intrusive method of collecting biometric exit data.

The Proposed Rule indicates that the use of valid passports by third parties has become more common given the increases in passport technology and related challenges in producing fraudulent documents.[2] CBP suggests that it has become easier for some individuals who wish to enter the United States unlawfully through ports of entry to do so by using a valid passport that belongs to someone else, rather than attempting to use a fake or altered passport. CBP even provides a number of anecdotal examples of such behavior that it claims were identified through its facial recognition pilot program at Washington Dulles International Airport.[3] However, CBP does not explain how those individuals would not have been detected by the myriad other protections described in the Proposed Rule already in place to identify these individuals.

For example, the sharing of airline reservation information with *all* governments is becoming an international treaty mandate. The International Civil Aviation Organization (ICAO) recently adopted an amendment to the Chicago Convention on Civil Aviation mandating that nearly every national government around the world require all airlines operating international flights to provide designated agencies with complete copies of all reservation records.[4] The Proposed Rule also confirms that the Aviation and Transportation Security Act and the Enhanced Border Security and Visa Entry Reform Act together mandate the collection of certain biographical manifest information on all passengers and crew members who arrive in or depart from the United States, and that this information is generally required to be transmitted to CBP.[5] This information is incredibly detailed, including the following: full name, date of birth, citizenship, passport/alien registration card number, travel document type, passport number, expiration date and country of issuance, alien registration number, country of residence, passenger name record locator number, and even a passenger's U.S. destination address.[6]

CBP therefore has access to an extraordinary amount of highly detailed information before passengers enter airports or board flights in the U.S. and abroad. Upon arrival in the U.S., however, there are

---

[1] *See, e.g.* Proposed Rule, 85 Fed. Reg. at 74167.
[2] *Id*.
[3] *Id*.
[4] Edward Hasbrouck, ICAO mandates worldwide government surveillance of air travelers, Papers Please, Sept. 2, 2020, *available at* https://papersplease.org/wp/2020/09/04/icao-mandates-worldwide-government-surveillance-of-air-travelers/.
[5] Proposed Rule, 85 Fed. Reg. at 74165.
[6] *Id*.

additional security and identify verification measures in place—including the collection of other biometric identifiers—that meaningfully address CBP's stated goal of preventing the use of valid passports by imposters. The Proposed Rule confirms that CBP collects fingerprints from travelers to biometrically verify their identity by comparing them to fingerprints collected previously in support of visa or immigration benefit applications, or prior inspection by CBP. This is in addition to the various other processes intended to verify a traveler's identity, including checking in with airlines and being evaluated by security personnel before they are allowed to board a flight to or from the U.S.

The Proposed Rule also repeatedly conflates biometric *entry* screening, including that of U.S. citizens who could opt-out under the rule, with biometric *exit* screening. For example, the Proposed Rule states that a total of two imposters were detected using facial recognition technology within two weeks of the technology being implemented at Washington Dulles International Airport. One of those individuals was an imposter arriving at Dulles on a U.S. passport who, under the Proposed Rule, would have been able to opt-out of screening.[7] The other was a Congolese national arriving on a French passport who was detected at primary inspection as he was entering the United States.[8] In addition, the Proposed Rule states that fully a third of all people detected by CBP using facial recognition technology deployed at the San Luis and Nogales ports of entry were travelling on U.S.-citizen passports, and thus would have been able to opt-out under the procedures in the rule.[9] That program was also an example of biometric entry screening, not biometric exit screening, which further undermines CBP's justification to impose facial recognition collection on tens of millions of people annually who are departing the United States and does not support CBP's justification of the rule on the basis of detecting visa overstays.

CBP also attempts to justify the imposition of sweeping new data collection based on a relatively small number of detected imposters. For example, over the two-week period in which two imposters were detected at Dulles Airport, more than 350,000 international passengers were processed at Dulles.[10] CBP does not explain in the rule why subjecting 350,00 people to intrusive facial recognition data collection is justifiable to detect the .0006 percent who may be imposters. Similarly, CBP states that a total of 138 imposters were detected in a pilot program deployed in fall 2018 at the San Luis and Nogales ports of entry, citing congressional testimony from July 10, 2019.[11] While CBP does not provide the total number of people subjected to facial recognition screening at those ports of entry, if we presume this technology was used only in pedestrian screening, from October 2018 to June 2019 a total of 4.32 million pedestrians entered the United States through those two ports of entry[12]—an imposter detection rate of .003 percent. If the technology were used on both pedestrians and personal vehicle passengers (13.3 million from October 2018 to June 2019), the imposter detection rate would fall to .001 percent.

---

[7] Customs and Border Protection, *Second Impostor in Three Weeks Caught by CBP Biometric Verification Technology at Washington Dulles Airport*, September 10, 2018, https://www.cbp.gov/newsroom/local-media-release/second-impostor-three-weeks-caught-cbp-biometric-verification.

[8] Customs and Border Protection, *CBP at Washington Dulles International Airport intercepted an imposter using new cutting-edge Facial Comparison Biometrics technology*, August 23, 2018, https://www.cbp.gov/newsroom/local-media-release/cbp-washington-dulles-international-airport-intercepted-imposter-using.

[9] Proposed Rule, 85 Fed. Reg. at 74167.

[10] Metropolitan Washington Airports Authority, *Air Traffic Statistics,* September 2018, https://www.mwaa.com/sites/default/files/09-18_ats_report_v3.pdf (over 700,000 international air passengers entered in September 2018).

[11] Proposed Rule, 85 Fed. Reg. at 74167.

[12] Department of Transportation, *Border Crossing Entry Data | Monthly Data*, https://explore.dot.gov/views/BorderCrossingData/Monthly.

Given the broad combination and expansive nature of the information provided to and collected by CBP, the infinitesimally small imposter detection rates, and the failure to consider that a significant portion of the detected imposters were travelling on U.S. passports and could opt-out of facial recognition screening, the agency's claim that subjecting millions of people—including U.S. citizens—to facial recognition is not justified, and can therefore not serve as a valid basis for the implementation of this sweeping Proposed Rule.

III. CBP proposes to expand biometrics collection using an unproven modality with significant privacy implications for citizens and noncitizens alike

CBP proposes to expand biometrics collection at all commercial ports of entry to include photographs for the specific use in facial recognition.[13] The Proposed Rule states that CBP has determined that facial recognition technology is currently the best available method for biometric verification, citing its purported accuracy and efficiency.[14] Despite rapid technological developments, significant concerns remain regarding the accuracy of facial recognition that undermine its stated purpose, as well as the secondary uses for such data. CBP has failed to meaningfully address these concerns, relying instead on conclusory statements regarding the current efficacy of the program as well as the best options available for improvement.

The Proposed Rule states that "certain privacy advocates" have expressed concern over the accuracy of facial matching technology especially as it relates to demographics such as age, race, and gender. While it is true that these concerns have been raised previously by individuals and non-governmental organizations, they are largely based on extensive and meaningful studies of the efficacy of facial recognition technology conducted by the federal government itself. For example, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has worked closely with the public and private sectors since the 1960s in assessing developments in biometrics technologies.[15]

NIST has conducted comprehensive testing of facial recognition technology platforms for over a decade and has found that, while the overall accuracy of these systems has improved in recent years, the rate of false positives and false negatives can vary widely depending on a person's gender, race, and age.[16] Of significant concern, NIST has found that the highest false positives are for people of African and Asian origin, and the lowest for people of eastern European origin.[17] NIST also found that the highest false negatives are for people born in Africa, Asia, and the Caribbean.[18] These findings, when combined with the knowledge that immigrants from Africa, Asia, and the Caribbean collectedly made up a full 47 percent of

[13] Proposed Rule, 85 Fed. Reg. at 74163.
[14] *Id*.
[15] Dr. Charles Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology, testimony before the U.S. House of Representatives, Committee on Homeland Security, February 6, 2020, *available at* https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0.
[16] *See* National Institute of Standards and Technology, Face Recognition Vendor Test, December 2019, p. 2, *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[17] *Id*.
[18] *Id*.

all immigrants that came to the United States in 2018,[19] undermine CBP's claim that facial recognition will serve as a more effective resource for identity verification than the current biometrics it collects. Critically, rather than addressing these concerns in detail, CBP instead makes the conclusory claim that they can be mitigated by "expanding the scope of individuals subject to facial image collection."[20] In other words, CBP's purported solution to addressing questions of accuracy in the use of facial recognition technology is to increase its use exponentially.

IV. CBP proposes to retain biometric information for as long as 75 years, creating significant privacy implications for U.S. citizens and noncitizens alike

The privacy risks associated with biometrics databases are extreme, with the greatest concerns relating to the breach or loss of personally identifiable information (PII) and the risk of misuse for large-scale surveillance. The Proposed Rule confirms CBP's intent to not only collect, but also retain sensitive biometric identifiers from millions of people annually for up to 75 years.[21] The risk of breaches or data loss relating to PII that CBP proposes to collect and store in perpetuity cannot be overstated given the government's demonstrated inability to retain such sensitive information securely. In the last five years alone, federal agencies, including CBP, have experienced a series of major breaches of large databases impacting millions of records. CBP must consider the costs of and lessons learned from these breaches when evaluating the Proposed Rule. The Proposed Rule disregards these considerations.

In 2015, the Office of Personnel Management was the subject of a breach that compromised 5.6 million fingerprints, social security numbers, and other personal information of more than 25 million people across the country.[22] Similarly, in 2019, DHS admitted that the images of nearly 200,000 people taken as part of a pilot program for its facial recognition program—the very same program that CBP cites in this Proposed Rule to support its claims of the purported value of facial recognition technology—was the subject of a cyberattack that resulted in the information being posted on the dark web.[23] This breach has been the subject of an investigation by the DHS Office of Inspector General (OIG) which culminated in a report and recommendations from the OIG to CBP on September 21, 2020[24]—just three months before the submission of this comment. While the report notes that CBP has agreed to all of OIG's recommendations, it remains highly unlikely that they have been fully implemented at this time. During the comment period, reporting revealed that suspected Russian hackers had penetrated DHS and other U.S. government agencies.[25] While the full scope of this sweeping cyberattack is still to be discovered, it

---

[19] Abby Budiman, Key Findings About U.S. Immigrants, Pew Research Center, August 20, 2020, *available at* https://www.pewresearch.org/fact-tank/2020/08/20/key-findings-about-u-s-immigrants/.
[20] Proposed Rule, 85 Fed. Reg. at 74175.
[21] Proposed Rule, 85 Fed. Reg. at 74191.
[22] U.S. Office of Personnel Management, Cybersecurity Resource Center: Cybersecurity Incidents, *available at* https://www.opm.gov/cybersecurity/cybersecurity-incidents/.
[23] Office of the Inspector General, U.S. Department of Homeland Security, Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot, September 21, 2020, p. 6, *available at* https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.
[24] *Id*.
[25] Reuters, *Suspected Russian hackers breached U.S. Department of Homeland Security – sources*, December 14, 2020, https://www.reuters.com/article/us-global-cyber-usa-dhs/suspected-russian-hackers-breached-u-s-department-of-homeland-security-sources-idUSKBN28O2LY.

further underlines the severe threat that hackers could obtain sensitive biometric details of millions of U.S. citizens and noncitizens that would be collected under the Proposed Rule.

Moreover, the consequences of such breaches often are not fully understood for years, given their scale and the relatively minimal understanding among the public of the information contained in federal government databases. Critically, the Proposed Rule makes no mention of the recent DHS breach, the OIG investigation, or related recommendations. DHS's plans to move forward with a dramatic expansion of biometrics collection under these conditions, while refusing to conduct a thorough analysis of the anticipated costs and likelihood of an information security breach, demonstrates a willful disregard of the privacy interests of millions of people and the impact that these breaches have on individuals.

V. The scale of collection and retention schedule outlined in the Proposed Rule raise serious concerns regarding secondary uses and general surveillance

The nature of facial recognition technology makes it highly susceptible to secondary uses and potential abuse. When combined with public video cameras, facial recognition technology can be used as a form of general surveillance. Moreover, it can be used in this manner passively and without the knowledge or consent of the parties impacted. When integrated with data from other governments and other government agencies—including the extraordinary increases in data collection that DHS proposed through a separate Proposed Rule earlier this fall[26]—the collection practices proposed in this Rule could allow DHS to build a database large enough to identify and track all people in public places, not just places DHS oversees, without their knowledge. Despite these concerns, the Proposed Rule does not provide any meaningful information regarding safeguards to prevent secondary uses and potential abuses.

The Proposed Rule also fails to specify the exact location where the department proposes to store the PII that it proposes to collect. While DHS has historically stored biometric data in its Automated Biometric Identification System (IDENT),[27] this new data will likely be stored in IDENT's replacement: DHS's new Homeland Advanced Recognition Technology (HART) database.

HART is currently the world's second largest biometrics collection and storage system,[28] and it is operated by the DHS Office of Biometric Identity Management and hosted by Amazon's GovCloud. According to HART's original privacy impact assessment, its records already include a wide array of information such as biometric data, biographic data, derogatory information such as warrants and immigration violations,

[26] U.S. Citizenship and Immigration Services, *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, 85 Fed. Reg. 56338 (September 11, 2020).
[27] U.S. Department of Homeland Security, DHS/OBIM/PIA-001 Automated Biometric Identification System, last updated November 14, 2019, *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.
[28] Chris Burt, *Inside the HART of the DHS Office of Biometric Identity Management*, BiometricUpdate.com, September 4, 2018, *available at* https://www.biometricupdate.com/201809/inside-the-hart-of-the-dhs-office-of-biometric-identity-management.

officer comment information, encounter data, and other unique machine-generated identifiers.[29] All of this additional PII will presumably be stored in its HART database, combined with millions of other entries, and stored by a third-party contractor. If that is the case, the PII of millions of individuals impacted by this Proposed Rule will be vulnerable to breach or future misuse given that it will all be stored together in a single database and using a unique identifier to link several different biometrics to each person forever.

VI. Violations of the Privacy Act

The data collection and retention practices detailed in the Proposed Rule will lead to repeated and ongoing violations of the Privacy Act of 1974 (Privacy Act).

The Privacy Act provides, in relevant part, that:

> "Each agency that maintains a system of records shall --... collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."[30]

The overarching goal of this statutory provision is simple—to help ensure the privacy and integrity of records and PII collected and maintained across the federal government. While CBP claims that it will comply with all legal requirements—including the Privacy Act—that govern the collection, use, maintenance, and disposition of PII in implementing the Proposed Rule, its plan for implementation and subsequent information-sharing agreements raise serious concerns about the veracity of its claims.[31]

CBP proposes to rely heavily on partners in the commercial travel industry to administer this new biometrics collection regime in an apparent effort to shift the considerable costs associated with its implementation. According to the proposed rule, CBP plans to enter into partnerships with carriers and airports to integrate facial recognition into the boarding process.[32] While the Privacy Act does leave room for exceptions to its requirements where collection by the federal government would not "practicable," CBP has failed to justify the proposed delegation of responsibilities to the private sector.

If CBP wishes to subject all international travelers to facial recognition, it can and should administer such a program directly, and it would be feasible for the agency to do so. As described in the Proposed Rule, CBP has conducted various facial recognition pilot programs at ports of entry in the past, and the purported success of these programs is used as a justification for the nationwide expansion of facial recognition.[33] Given these prior initiatives, it is conceivable that CBP could increase capacity on its own over time. CBP instead claims that the proposed arrangement will create the greatest 'convenience' for travelers, airlines, and the government in justifying the proposed extensive involvement of entities and

---

[29] U.S. Department of Homeland Security, Privacy Threshold Analysis for Homeland Advanced Recognition Technology, April 2015, at 16, *available at* https://epic.org/foia/dhs/hart/EPIC-2018-06-18-DHS-FOIA-20190422-Production.pdf.

[30] 5 U.S.C. §552a(e)(2).

[31] *See* Proposed Rule, 85 Fed. Reg. at 74164.

[32] Proposed Rule, 85 Fed. Reg. at 74184.

[33] *See* Proposed Rule, 85 Fed. Reg. at 74167.

individuals outside of the federal government in administering this new program.[34] Such a justification is wholly insufficient given the nature and scope of the Proposed Rule.

The true justification for CBP's effort to shift its responsibilities to the private sector in this manner appears to be the related and significant cost savings to the agency that will make full, nationwide implementation possible in a relatively short period of time. The considerable hardware costs associated with the collection and transmission of facial images will be borne by the carriers and airports who partner with CBP.[35] Despite the expense, the Proposed Rule indicates that CBP expects to be able to implement the program nationwide within just five years.[36] It is reasonable to wonder why CBP's partners in the private sector—for-profit entities—would be willing to accept these considerable costs, and implement this program in such a short period of time when not otherwise required by law. It appears that CBP hopes to incentivize such collaboration by providing access to its facial recognition database to its commercial partners for their own business purposes.[37] CBP is, in essence, planning to induce the airline industry into implementing this sweeping new facial recognition program in exchange for 'free' use of the same service.

Despite the concerning nature of such an arrangement, the Proposed Rule fails to detail the scope and nature of this access, or any details relating to any privacy protections and limitations for the carriers that would be able to access CBP's database(s). The Privacy Act, for good reasons, does not permit such a scheme. The collection and storage of sensitive biometric information is, and should remain, strictly a governmental function. If CBP wishes to collect more biometric information from travelers, it must do so directly. The Proposed Rule must be withdrawn or revised.

VII. Chad Wolf, the Purported Acting Secretary of the Department of Homeland Security, Was Unlawfully Appointed and Does Not Have Authority to Promulgate This Regulation

The Proposed Rule, which is signed by Acting DHS General Counsel Chad Mizelle following a delegation of authority by purported Acting Secretary Chad Wolf, is void *ab initio* because Mr. Wolf is not the lawful Acting Secretary of DHS.

On December 9, 2016, President Barack Obama issued Executive Order 13753, establishing the default order of succession at DHS "[i]n case of the Secretary's death, resignation, or inability to perform the functions of the Office."[38] Under this Executive Order, the CBP Commissioner was seventh in line for succession in the case of the Secretary's resignation, after both the Under Secretary for National Protection and Programs and the Under Secretary for Intelligence and Analysis.

On April 10, 2019, DHS Secretary Kirstjen Nielsen exercised her authority to amend the order of succession, issuing a memorandum delegating a new line of succession "in the event I am unavailable to

[34] *See* Proposed Rule, 85 Fed. Reg. at 74170.
[35] Proposed Rule, 85 Fed. Reg. at 74184.
[36] Proposed Rule, 85 Fed. Reg. at 74181.
[37] *See* Proposed Rule, 85 Fed. Reg. at 74174.
[38] President Barack Obama, Executive Order 13753, Amending the Order of Succession in the Department of Homeland Security, 81 Fed. Reg. 90.667, December 9, 2016.

act during a disaster or catastrophic emergency."[39] This memorandum did *not* change the line of succession, however, "in the case of … resignation," making clear that following a resignation, "the orderly succession of officials is governed by Executive Order 13753, amended on December 9, 2016."[40] Secretary Nielsen then resigned that same day.

Following Secretary Nielsen's resignation, the next in line successor for the Acting Secretary role, under her memorandum and Executive Order 13753, was the Under Secretary for National Protection and Programs. Nevertheless, DHS installed the CBP Commissioner, Kevin McAleenan, as the Acting Secretary of DHS. Mr. McAleenan served as purported Acting Secretary through November 2019, when he attempted to once again amend the line of succession to allow Mr. Wolf, then Under Secretary for Strategy, Policy, and Plans, to serve as Acting Secretary following his own resignation.[41] Given that Mr. Mr. McAleenan's appointment was made in violation of Executive Order 13753, his attempt to amend the DHS line of succession in this manner was unlawful.

Moreover, this action occurred more than 210 days following Secretary Nielsen's resignation, meaning that even if Mr. McAleenan was properly designated as Acting Secretary on April 10, 2019, under the Federal Vacancies Reform Act and not the Homeland Security Act, by November 8, 2019, he no longer held that authority and could not have lawfully exercised the authority of an Acting Secretary to amend the DHS line of succession.[42] Given these revelations, a number of federal courts have held that Mr. Wolf is not lawfully serving as the acting Secretary of DHS under either the Homeland Security Act or the Federal Vacancies Reform Act.[43] The U.S. Government Accountability Office has come to the same conclusion.[44] Mr. Wolf therefore has neither the lawful authority to sign the proposed rule, or to delegate such authority to others. The Proposed Rule is void *ab initio* and must be withdrawn.

VIII. Insufficient Comment Period

The Council notes that DHS failed to provide a sufficient period for interested parties to comment on this Proposed Rule. Under most circumstances, agencies must provide public comment periods of at least 60

---

[39] *See* DHS Orders of Succession and Delegations of Authorities for Named Positions, DHS Delegation No. 00106, Updated April 10, 2019, *available at* https://oversight.house.gov/sites/democrats.oversight.house.gov/files/191115%20T%20Dodaro%20re%20Letter%20to%20GAO%20on%20Wolf-Cuccinelli%20Appointment.pdf.

[40] *Id*.

[41] *See* Kevin McAleenan, "Amendment to the Order of Succession for the Secretary of Homeland Security," November 8, 2019, *available at* https://oversight.house.gov/sites/democrats.oversight.house.gov/files/191115%20T%20Dodaro%20re%20Letter%20to%20GAO%20on%20Wolf-Cuccinelli%20Appointment.pdf.

[42] *See* 5 U.S.C. § 3346(a)(1) ("Except in the case of a vacancy caused by sickness, the person serving as an acting officer as described under section 3345 may serve in the office … for no longer than 210 days beginning on the date the vacancy occurs").

[43] *Casa de Maryland, Inc. v. Wolf*, ––– F. Supp. 3d ––––, 20-cv-2119, 2020 WL 5500165 (D. Md. Sept. 11, 2020) and *Immigrant Legal Res. Ctr. v. Wolf*, ––– F. Supp. 3d ––––, 2020 WL 5798269 (N.D. Cal. Sept. 29, 2020).

[44] *See* U.S. Government Accountability Office, *Legality of Service of Acting Secretary of Homeland Security and Service of Senior Official Performing the Duties of Deputy Secretary of Homeland Security*, August 14, 2020, available at https://www.gao.gov/assets/710/708830.pdf.

days in length.[45] There is no evidence that 60 days would be unfeasible or unlawful in the present case, but DHS nevertheless elected to limit the comment period to 30 days. This rushed 30-day comment period is inappropriate given the sweeping implications of this Proposed Rule, the ongoing coronavirus pandemic, and the looming transition in presidential administrations.

The Proposed Rule is 99 pages in length and includes significant changes with broad privacy and economic implications for individuals and the federal government alike. Additionally, many individuals interested in commenting on this Proposed Rule are dealing with unanticipated and emergent matters resulting from the pandemic, limiting their ability to do so. The insufficient comment period prevented the Council from being able to provide a complete analysis of several additional issues including the following:

- The Proposed Rule would violate the Paperwork Reduction Act as it relates to the required or authorized collection of information from U.S. citizens.[46]

- The Proposed Rule's impact assessment is inaccurate as it fails to meaningfully account for the economic cost to individuals who opt out of collection and subsequently miss their flight due to related delays in the alternative screenings outlined by CBP.

- The Proposed Rule seeks to eliminate the age requirement for collection of biometric information. CBP's justification for eliminating age restrictions on biometrics fails to justify its departure from current practice and fails to consider the effects of puberty and aging on biometric capture for children.

For these reasons, we call on DHS to withdraw the proposed rule and provide at least an additional 30 days to comment.

IX. Conclusion

The Council opposes the Proposed Rule as it constitutes an improper invasion of privacy that is unnecessary to achieve DHS's stated objectives. It therefore represents an impermissible infringement upon the rights of U.S. citizens and noncitizens alike. We therefore respectfully urge DHS to rescind the Proposed Rule and withdraw it from consideration.

Sincerely,

American Immigration Council

[45] *See, e.g.*, Exec. Order 12866, 58 Fed. Reg. 51735 (Oct. 4, 1993) (directing agencies generally to furnish "not less than 60 days" for public comment); Exec. Order 13563, 76 Fed. Reg. 3821 (Jan. 21, 2011) ("To the extent feasible and permitted by law, each agency shall afford the public a meaningful opportunity to comment through the Internet on any proposed regulation, with a comment period that should generally be at least 60 days.").

[46] *See* 44 U.S.C. §3501-3521.