Privacy Impact Assessment
for the

Department of Homeland Security (DHS) Immigration-Related Information Sharing with U.S. Census Bureau

DHS/ALL/PIA-079

December 20, 2019

Contact Point
Marc Rosenblum
Deputy Assistant Secretary
Office of Immigration Statistics
Department of Homeland Security

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

Pursuant to Executive Order (E.O.) 13880 *Collecting Information About Citizenship Status in Connection with the Decennial Census*, issued July 11, 2019, the Department of Homeland Security (DHS) is providing the Department of Commerce (DOC), U.S. Census Bureau (Census or Census Bureau) with administrative records to assist in determining the number of citizens, lawfully present non-citizens, and unauthorized immigrants in the United States during the decennial census (2020 Census). DHS will share various data elements that the Census Bureau has articulated a need to know for the purpose of executing the E.O., including personally identifiable information (PII), with Census to (1) update 2020 Census person files, (2) produce Citizen Voting Age Population Statistics, and (3) conduct testing of citizenship models. DHS is publishing this Privacy Impact Assessment (PIA) to describe the establishment of a formal Memorandum of Agreement (MOA) between DHS and the Census Bureau and to analyze the collection, use, and dissemination of DHS information by Census.

Introduction

As part of its mission to safeguard the American people, homeland, and values, DHS collects, maintains, and shares a vast amount of personally identifiable information. DHS maintains information about individuals seeking to immigrate to the United States, individuals seeking lawful entry to the United States, and individuals in violation of U.S. immigration law, among others. Three DHS components work in close coordination to ensure the safety and security of the United States while facilitating lawful travel, immigration, and trade. U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States and is responsible for processing petitions and applications for immigration benefits, as well as other immigration-related requests. U.S. Customs and Border Protection (CBP) is responsible for securing the United States and its borders while facilitating lawful travel and trade. U.S. Immigration and Customs Enforcement (ICE) enforces more than 400 federal statutes and focuses on immigration enforcement, preventing terrorism, and combating the illegal movement of people and goods.

Necessarily, DHS components USCIS, CBP, and ICE, collect and maintain a considerable amount of information about individuals in various stages of the lawful immigration and lawful nonimmigrant processes, as well as individuals encountered as part of border security and immigration enforcement actions. As the unified United States immigration and border security Agency, DHS's ability to determine an individual's citizenship is a critical part of many DHS enforcement actions and benefit determinations.

Determining an individual's citizenship based on various DHS data is a challenging task. USCIS maintains the final benefit determinations of whether an individual has been granted status

as a Lawful Permanent Resident (LPR) or a naturalized U.S. citizen. Beyond those two immigration benefit determinations, CBP and ICE determine lawful status of individuals previously admitted into the United States and whether they have overstayed the terms of admission (known as an "overstay"). Determining an individual's lawful status in the United States requires more than solely matching entry and exit travel data. For example, a person may receive from CBP a six-month admission upon entry, and then he or she may subsequently apply for and receive from USCIS an extension of up to six months. Identifying extensions, changes, or adjustments of status are necessary steps to determine whether a person has overstayed their authorized period of admission.

Due to the decentralized nature of admission and immigration information, as well as the lack of a nationwide departure control system, CBP collects different data points from different data sets to create a "complete travel history" of an individual traveler. USCIS, CBP, ICE, and other DHS components contribute to the Arrival and Departure Information System (ADIS),[1] which generates an implied immigration status of an individual based on the date he or she entered the United States; class of admission; updates or changes to his or her immigration status; and, when available, the date he or she departed the United States.

Due to complexity and overlap of travel, immigration, and enforcement records, DHS typically confines its sharing and uses of citizenship-related information to the enforcement of U.S. laws and the facilitation of benefit determinations. However, pursuant to Executive Order (E.O.) 13880: *Collecting Information About Citizenship Status in Connection with the Decennial Census*,[2] DHS will now also provide citizenship and immigration benefits information about individuals to the U.S. Census Bureau. Though the development of this sharing effort by USCIS, CBP, and ICE represents a new initiative for DHS, USCIS has been providing anonymized data on LPRs and naturalized citizens to Census annually since at least 2007. DHS memorialized this information sharing arrangement through a MOA with the Census Bureau.

Census Bureau Use of DHS Citizenship Data

The U.S. Census Bureau is the Federal Government's largest statistical agency and provides current facts and figures about the people and economy of the United States. Census collects data about the economy and the people present in the United States from many different sources, including directly from respondents through decennial censuses and surveys, and from other sources including federal, state, and local governments, as well as some commercial entities. Data from other sources is called "administrative data" because this data was originally collected

[1] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* www.dhs.gov/privacy.
[2] E.O. 13880: *Collecting Information About Citizenship Status in Connection with the Decennial Census*, 84 FR 33821 (July 11, 2019).

by other federal and state agencies to administer programs and provide services to the public.[3] Census is required by law to obtain and reuse data that already exists at other agencies to reduce the burden on people who respond to census and survey questions.[4] By reusing data that already exists elsewhere, and linking it to census and survey data, Census is able to conduct research that provides a more holistic view of the people present in, and the economy of, the United States. The Census Bureau will use the data for research and operations to improve record linkage methods for surveys, including the decennial census. Research and operations are terms used to describe the statistical work that the Census Bureau conducts as part of collecting data, linking data, and producing and publishing estimates. Linked data also assist researchers in answering questions that could not be answered using one data set, as well as help other government agencies better understand how their programs are working, and where they could be improved.[5]

Research Projects

1. Update 2020 Census Person Files

In order to approximate coverage of the population in support of its statistical programs, the Census Bureau will acquire administrative record files from DHS and agencies such as the Departments of Agriculture, Education, Health and Human Services, Housing and Urban Development, Labor, Treasury, Veterans Affairs, the Office of Personnel Management, the Social Security Administration, the Selective Service System, and the U.S. Postal Service. Comparable data may also be sought from state agencies and commercial sources and websites.

Person records in each administrative and survey data source, including the 2020 Census, will be validated and assigned a unique person identifier, called a Protected Identification Key (PIK). The PIKs will be used to link each person's citizenship information to their 2020 Census record. The validation process (called the Person Identification Validation System (PVS)) involves comparing records to federal government sources (reference files) using fields such as Social Security number (SSN), name, date of birth, sex, and residential address. Several million U.S. residents do not have either an SSN or an Individual Taxpayer Identification Number (ITIN).[6]

---

[3] 13 U.S.C. § 6 provides the legal authority for Census to receive administrative data from federal departments and agencies pertinent to its work.

[4] A census collects information about every member of the population – a census is a 100 percent sample survey. A survey is a data collection activity involving a sample of the population.

[5] Linked data or Linked files are files produced when DHS Data is processed through the Census Bureau's Person Identification Validation System (PVS) to assign a unique identifier (protected identification key (PIK)). The Linked Files are further separated into two distinct files: (a) Linked Name File – File containing the PIK and names from the Source Data; and (b) Linked Research File – File containing PIK, and when linked on PIK: demographic data, geographic data, mortality data, health data, and economic data. Records are extracted or combined as needed using the unique non-identifying codes, not by name or SSN, to prepare numerous statistical products.

[6] An Individual Taxpayer Identification Number (ITIN) is a tax processing number issued by the Internal Revenue Service (IRS). The IRS issues ITINs to individuals who are required to have a U.S. taxpayer identification number but do not have, and are not eligible to obtain, an SSN. *See* https://www.irs.gov/individuals/individual-taxpayer-identification-number.

DHS Source Data will assist the Census Bureau in creating the project reference files it will use in PVS for those individuals in the 2020 Census without an SSN or an ITIN. DHS data should reduce the number of people in the 2020 Census who cannot be assigned PIKs and thus have little information to inform their modeled probability of being a citizen or a lawfully present non-citizen.

2. Produce Citizen Voting Age Population Statistics

Once citizenship and immigration status data sources and the 2020 Census person file have been assigned PIKs, the citizenship and immigration data will be linked to the 2020 Census person file. A model will be estimated for each person with a PIK, using the most current citizenship status from each available citizenship source for the person, as well as the person's other demographic, household, and location information as explanatory variables. The model will produce a citizenship probability for each person, which will then be combined with age, race, ethnicity, and location information from the 2020 Census to produce the Citizen Voting Age Population (CVAP) statistics. The objective of the project is to determine the number of citizens and non-citizens in the country.

The administrative records data will both expand the coverage of persons with citizenship and immigration information in the 2020 Census and provide more up-to-date citizenship and immigration status estimates for those already covered by other sources, resulting in more accurate statistics about the U.S. population.

3. Testing

Prior to producing citizenship statistics in the fall/winter of 2020-2021, the Census Bureau will do extensive testing of the citizenship models. Researchers will use past censuses and the American Community Survey (ACS)[7] as person frames (in place of the 2020 Census), together with citizenship information from administrative sources in the same time periods. The testing will require historical data.

Data Provided by USCIS and CBP[8]

DHS plans to provide information to Census by extracting information from USCIS and CBP systems and ensuring that the data provided is as timely and accurate as possible. USCIS and CBP will separately transmit data to Census. A description of the specific data sources, data elements, and transmission process is included as Appendices to this PIA. Should Census seek additional data elements in the future, DHS will analyze the privacy implications of sharing that information in an update to this PIA and/or its appendices.

[7] More information about the ACS is available at https://www.census.gov/programs-surveys/acs.
[8] CBP will facilitate the transfer of ICE data elements for the Census sharing initiative.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that this is an information sharing arrangement rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This PIA examines the privacy impact of DHS and Census information sharing as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

The Privacy Act of 1974[9] permits agencies to disclose information from a system of records to the Census Bureau "for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13."[10] Additionally, the recently published Executive Order[11] provides notice to the public about what administrative data must be provided to the Census Bureau. Lastly, the Census Bureau itself has a considerable amount of information on their public-facing website about administrative and third-party information that Census uses to conduct survey and statistical operations.[12]

Although some DHS datasets are explicitly mentioned in the Executive Order, DHS is

[9] 5 U.S.C § 552a.
[10] 5 U.S.C § 552a(b)(4).
[11] E.O. 13880: *Collecting Information About Citizenship Status in Connection with the Decennial Census*, 84 FR 33821 (July 11, 2019).
[12] https://www.census.gov/about/what/admin-data.html.

providing additional notice and transparency regarding Census use of DHS data through this PIA to imply or attach citizenship or immigration status information to respondent records.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Data provided in support of this MOA will be shared from DHS source systems. For the most part, DHS collects information maintained in their respective source systems directly from the individual seeking an immigration benefit or entry to the United States. DHS maintains accurate and up-to-date information and ensures that individuals are properly notified at the time of collection that their information will be maintained in Departmental information systems, used for a variety of purposes, and disseminated as necessary. Individuals are not offered the opportunity to opt out of DHS's sharing with the Census Bureau.

DHS provides U.S. citizens and Lawful Permanent Residents with the opportunity to access and seek amendment to their information maintained in the respective source systems through the submission of Privacy Act or Freedom of Information Act (FOIA) requests. Individuals not covered by the Privacy Act may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Individuals seeking access to or amendment of their records may submit a request in writing to the DHS Chief Privacy and FOIA Officer at:

Chief Privacy Officer and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
245 Murray Drive, SW, Building 410, STOP-0655
Washington, D.C. 20528

Privacy Risk: There is a risk that an individual cannot correct or amend information about them that is used by Census.

Mitigation: This risk cannot be fully mitigated. While the data provided by DHS will not be used to make programmatic or administrative enforcement decisions, the Department endeavors to maintain, use, and share the most accurate, relevant, timely, and complete records possible. Additionally, the MOA between DHS and Census specifically notes that all information, including PII shared under this agreement shall, to the extent feasible, be as accurate, complete, and current as necessary. As most of the information shared under this agreement is collected directly from the individual or his or her representative, it is assumed to be accurate at the time it was collected. However, because DHS is providing information at a point in time, it is reasonable to believe that eventually data accuracy issues may arise.

This PIA provides notice of the Department's redress process to individuals whose information is shared by DHS to Census. That process allows for individuals to amend erroneous information maintained by DHS. Census has exempted records contained in COMMERCE/CENSUS-8 Statistical Administrative Records System from access and amendment pursuant to 5 U.S.C. § 552a(k)(4).[13]

Privacy Risk: There is a risk that individuals were not aware at the time of collection that their information would be shared with the Census Bureau and may not want their information shared.

Mitigation: This risk is not mitigated. There is no opportunity to consent to sharing or opt out of having an individual's information shared with the Census Bureau. DHS is required under E.O. 13880 to provide the requested information to Census. While some notice of the potential for sharing is provided through the Privacy Act, it is not clear to an individual that an agency will share for those purposes even though it is permitted to do so.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The legal authority for the Census Bureau to enter into an information sharing access agreement with DHS is 13 U.S.C. § 6, which permits the Census Bureau to access, by purchase or otherwise, information to assist the Census Bureau in the performance of duties under Title 13, United States Code.

The legal authority for DHS to enter into this Agreement is 6 U.S.C § 112(b)(2). Additionally, 5 U.S.C. § 552a(b)(4) permits DHS to share Privacy Act-protected records with the Census Bureau for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13 provided a "need to know" the specific information requested is identified. Other authorities that govern and limit the sharing of information between DHS and the Census Bureau include the following:

1. 5 U.S.C. § 552a, Privacy Act of 1974; to include relevant system of records notices (SORNs);
2. 8 U.S.C. § 1367;
3. 8 C.F.R. 208.6;
4. 8 U.S.C. § 1254a and 8 CFR § 244.16;
5. Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62;

[13] COMMERCE/CENSUS-8 Statistical Administrative Records System, 81 FR 76554 (Nov. 3, 2016), *available at* http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-8.html.

6. GPRA Modernization Act of 2010, Pub. L. No. 111-352; and
7. OMB Memoranda M-15-15, "Improving Statistical Activities through Interagency and Collaboration" (July 8, 2015).

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

DHS and Census coordinated during the development of the MOA to ensure that the Department sends the minimum amount of information necessary to support the Census projects. The MOA developed by DHS and Census outlines the specific agreed-upon data elements that will be provided.

All original, unaltered DHS Source Data will be retained by the Census Bureau no more than two years after receipt from DHS. The Census Bureau will also match all DHS administrative records to survey respondent information. These linked data[14] will be included as part of the subject record matching the assigned Census identifier and will be retained by Census for two years or until no longer required for programmatic purposes, whichever is longer.[15] The Census Bureau's use of this data is governed by the MOA with DHS governing this disclosure of information and the data will be retained consistent with the COMMERCE/CENSUS-8, Statistical Administrative Records System.[16]

Census will provide DHS with notification within 30 days of the completion of the research and request authorization to destroy the data it was provided. Written notification provided by Census will certify that the data has been destroyed and that no parts thereof will be retained without the express written permission of DHS. To ensure compliance with established retention and disposal requirements, DHS will work with Census to develop and implement a review and assessment process, including the conduct of annual self-audits by Census, which will be provided to DHS.

[14] Note that Census' linking method assigns a match probability score of zero to one to every DHS administrative record; records are retained in the linked dataset regardless of their scores.
[15] *See* DAA-0029-2014-0005, Records of the Center for Administrative Records Research and Applications, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg-0029/daa-0029-2014-0005_sf115.pdf.
[16] *See* COMMERCE/CENSUS-8, Statistical Administrative Records System, 81 FR 76554 (Nov. 13, 2016), *available at* http://www.osec.doc.gov/opog/PrivacyAct/SORNs/census-8.html.

Privacy Risk: There is a risk that Census will retain DHS information for longer than necessary.

Mitigation: This risk is not mitigated. Census will retain the original DHS administrative data for a maximum of two years from the date of receipt pursuant to DAA-0029-2014-0005, with the ability to destroy data sooner if it is no longer necessary for analytical projects. All data run through the PVS process is considered linked data. All linked or derivative files will be retained by Census for two years or until no longer required for programmatic purposes, whichever is longer. Because this is a new use, DHS has no way to estimate how long Census will require the files for programmatic purposes.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The Census Bureau plans to use several administrative data sources of citizenship and immigration status in a statistical model that will produce a probability of being a U.S. citizen, a lawfully present non-citizen, or an unauthorized immigrant on April 1, 2020, for each person in the 2020 Census. The citizenship and immigration status probabilities will be used together with age, race, ethnicity, and location information from the 2020 Census to produce CVAP statistics. The objective of the project as described in the E.O. is to determine the number of citizens, lawfully present non-citizens, and unauthorized immigrants in the country.

Person records in each administrative and survey data source, including the 2020 Census, will be validated and assigned a unique person identifier, called a PIK. The PIKs will be used to link each person's citizenship information to his/her 2020 Census record. The validation process (the PVS) involves comparing records received by the Census Bureau to reference files using fields such as SSN or ITIN, name, date of birth, gender, and residential address. Several million U.S. residents do not have either an SSN or an ITIN. Thus, DHS Source Data will assist the Census Bureau in creating the project reference files it will use in PVS for those individuals in the 2020 Census without an SSN or an ITIN.

Once citizenship data sources and the 2020 Census person file have been assigned PIKs, the citizenship data will be linked to the 2020 Census person file. A model will be estimated for each person with a PIK, using the most current citizenship status from each available citizenship source for the person, as well as the person's other demographic, household, and location information as explanatory variables. The model will produce a citizenship and immigration status probabilities for each person, which will then be combined with age, race, ethnicity, and location information from the 2020 Census to produce the CVAP statistics.

Prior to producing citizenship statistics in the fall/winter of 2020-2021, the Census Bureau will do extensive testing of the citizenship models. Researchers will use past censuses and the American Community Survey (ACS) as person frames (in place of the 2020 Census), together with citizenship information from administrative sources in the same time periods. The testing will require historical data.

The administrative records data will both expand the coverage of persons with citizenship and immigration status information in the 2020 Census and provide more up-to-date citizenship and immigration status information for those already covered by other sources, resulting in more accurate statistics about the U.S. citizen population.

Privacy Risk: There is a risk that Census may use the DHS data for unauthorized purposes.

Mitigation: This risk is mitigated. Census's use of this data is limited to only those projects that have been approved by DHS and described in this PIA. Additionally, Census limits access to DHS information to staff with a valid need-to-know, and a limited number of individuals with special sworn status (SSS).[17] 13 U.S.C. § 214 and 18 U.S.C. §§ 3551, 3559, and 3571 provide for the imposition of penalties of up to five years in prison and/or up to $250,000.00 in fines for wrongful disclosure of confidential census information.

Privacy Risk: There is a risk that the Census Bureau's use of the DHS data is not compatible with the original purpose of collection by DHS.

Mitigation: This risk cannot be mitigated. E.O. 13880 requires DHS to share information requested by the Census Bureau regardless of whether the sharing is compatible with the original purpose of the collection. The Privacy Act does not prohibit the sharing. The Privacy Act permits disclosure to the U.S. Census Bureau pursuant to 5 U.S.C. 552a(b)(4) "for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13."

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The accuracy of the information shared with Census depends on the accuracy and quality of data from each DHS source system. As most of the information shared under this agreement is collected directly from the individual or his or her representative, it is assumed to be accurate at the time it was collected. As noted above, DHS offers individuals the ability to correct their information within the respective USCIS and CBP source systems. Any corrections made by an individual prior to the data transmission to Census will be reflected in the source system. However,

[17] Individuals who are granted Special Sworn Status (SSS) pursuant to 13 U.S.C. § 23(c) (SSS Researchers), may be permitted access to linked and derivative data within a secure restricted-access environment.

in the event an individual makes updates and/or corrections to the data after the information is shared with Census, the individual's updated information will not be shared with Census.

Privacy Risk: There is a risk that Census will inaccurately link the DHS data to the Census data received from other sources.

Mitigation: This risk cannot be fully mitigated. Linking records between datasets is not likely to be 100% accurate. However, Census will develop an imputation system for the citizenship and immigration status variable and will employ methodologies to ensure that PII is protected. In particular, Census intends to take data obtained from DHS and match it against data it receives from sources such as the Social Security Administration and the U.S. Department of State. For these particular sources, the SSN will be used as the common identifier, when available. If there are duplicate identities found using the SSN or ITIN, Census will use the Alien Registration Number as one potential source to distinguish one identity from another. Once all data related to an individual is gathered, the information will be anonymized and provided a unique identifier created by Census. The Census Bureau, upon discovery of data quality errors in the original, unaltered source DHS files will promptly notify DHS so that corrective action may be taken, if and as necessary.

Furthermore, the data linking procedures help to ensure an overall quality to the data that allows statistical and not operational use. Because the data is not used to make any operational decisions, the impact of inaccurately linking the data is low.

Privacy Risk: There is a risk that Census will assign an inaccurate immigration status to an individual.

Mitigation: This risk is partially mitigated. As noted previously, immigration status information is challenging, complicated, and dynamic. Once citizenship data sources and the 2020 Census person file have been assigned PIKs, the citizenship data will be linked to the 2020 Census person file. A model will be estimated for each person with a PIK, using the most current citizenship or immigration status information from each available source for the person, as well as the person's other demographic, household, and location information as explanatory variables. The model will produce a citizenship and immigration status probability for each person, which will then be combined with age, race, ethnicity, and location information from the 2020 Census to produce the CVAP statistics. The CVAP file will only provide a percentage of each citizenship and immigration status aggregated at the block level geography. Therefore, no one will be able to determine if an inaccurate citizenship or immigration status was assigned to an individual.

No one source of citizenship information is complete and up-to-date. The SSA Numident[18] contains citizenship status for most of the population but the information is not always up to date

[18] *See* SSA 60-0058, Master Files of Social Security Number (SSN) Holder and SSN Applications, 75 FR 82121 (Dec. 29, 2010), *available at* http://www.ssa.gov/privacy/sorn.html.

for foreign-born persons. Prior to the 1970s people were not required to provide evidence of citizenship status when applying for an SSN. Thus, the citizenship status is blank for many older people in the Numident. Also, naturalized citizens are not required to notify SSA about their naturalization. Thus, a naturalized citizen's SSA record may incorrectly say the person is not a citizen. Individuals who derive citizenship when their parent(s) naturalize also may choose to not obtain a citizenship certificate from USCIS but rather apply for an SSN or a passport to establish proof of their citizenship.[19] To the extent that Census mis-applies an individual's citizenship status, it is for statistical purposes and Census statistical products only. There will be no adverse impact to the individual record subject.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The Census Bureau is responsible for ensuring the data security, integrity, and confidentiality of DHS records after they are supplied to the Census Bureau, and for maintaining safeguards to prevent any unauthorized disclosure of the data. The Census Bureau is committed to respecting respondent privacy and protecting confidentiality. Through the Data Stewardship Program, the Census Bureau has implemented management, operational, and technical controls and practices to ensure high-level data protection for respondents of our censuses and surveys.

- An unauthorized browsing policy protects respondent information from casual or inappropriate use by any person with access to Title 13 protected data.
- All Census Bureau employees, persons with special sworn status, as well as employees of FedRAMP-approved cloud services who may have incidental access to Title 13 protected data, are subject to the restrictions, penalties, and prohibitions of 13 U.S.C. §§ 9 and 214; 18 U.S.C. §§ 3551, 3559, 3571; the Privacy Act of 1974 (5 U.S.C. § 552a(g) and (i); 18 U.S.C. § 1905; 26 U.S.C. §§ 7213, 7213A, and 7431; and 42 U.S.C. § 1306.
- All Census Bureau employees and persons with special sworn status will be regularly advised of regulations issued pursuant to Title 13 governing the confidentiality of the data, and will be required to complete an annual Data Stewardship Awareness training. The restricted-access IT environment has been established to limit the number of Census Bureau staff with direct access to the personal identifiers in this system to protect the confidentiality of the data and to prevent unauthorized use or access. These safeguards provide a level and scope of security that meet the level and scope of security established

[19] The N-600 Application for Certificate of Citizenship currently carries a filing fee of $1,170, though some individuals may qualify for a fee waiver (Form I-912). Alternatively, a passport card can be obtained for a child for $50 to $65, depending on the age of the child.

by OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources.

- All Census Bureau and FedRAMP-approved computer systems that maintain sensitive information are in compliance with the Federal Information Security Modernization Act, which includes auditing and controls over access to restricted data.
- The use of unsecured telecommunications to transmit individually identifiable information is prohibited.
- Paper copies that contain sensitive information are stored in secure facilities in a locked drawer or file cabinet behind a closed door.
- Any publications based on the Statistical Administrative Records System will be cleared for release under the direction of the Census Bureau's Disclosure Review Board, which will confirm that all the required disclosure protection procedures have been implemented. No information will be released that identifies any individual. Noise injection is the Census' preferred disclosure avoidance technique. By policy, noise injection is to be applied to all data products that are reported with geographies smaller than a state. In cases when it is not feasible to fully implement noise injection within the period of the contract, a transition plan for implementing noise injection or other provable privacy methods must be developed in coordination with the Census. Noise injection may be required for microdata releases, depending on the characteristics of the microdata and the specific variables that are to be released.

Specific Data Transfer Protections

When files are acquired and transmitted to Census, they are initially accessible only by a small staff of Census Bureau employees responsible for inventorying the contents of the file, conducting basic Quality Control checks, and removing sensitive PII. This staff works in a secured physical environment and on a highly-restricted computing cluster that is behind the Census firewall.

The processing and de-identification staff confirms that the received files are exactly as described in the legal agreement. Census is never permitted to receive more than has been specified in the applicable agreement. The staff also confirms that the variables and documentation have a basic integrity that will allow the U.S. Census Bureau to use them.

Next, a data linkage team replaces sensitive PII with a unique key that can be used to link the records to other databases held at Census. The probabilistic linkage process relies on variables such as name, address, date of birth, and Social Security number. These variables are used to link the incoming file to a "reference file" comprised of censuses, surveys, and other federal records. The reference file contains PII from these other files and a PIK, which uniquely identifies each

record. When a linkage can be made between the incoming file and the reference file, the PIK is appended to the incoming file.

DHS will transfer the data to Census via a Secure File Transfer Protocol (SFTP). SFTP is a network protocol for transferring files securely over a computer network via encryption. SFTP is a set of commands that runs over another protocol known as Secure Shell (SSH). SSH consists of many layers including a transport layer, a user authentication layer, and a connection layer. SSH is a Federal Information Processing Standard 140-2-approved Internet Engineering Task Force protocol, which provides encrypted connections and supports authentication with digital certificates and other secure methods of authentication.[20]

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Pursuant to the MOA between DHS and Census, the Department reserves the right to make onsite inspections and to monitor and review all records and documents related to the use, or the suspected or confirmed improper use of DHS data shared or suspected or confirmed breaches of DHS data held by Census during the lifetime of the agreement.

Privacy Risk: There is a risk that Census and SSS employees are not trained on how to properly handle DHS data.

Mitigation: This risk is mitigated. Census and SSS employees receive training on the specific use and purpose in sharing this data as well as training on privacy compliance, the handling of PII, the confidentiality of records, the safeguards required to protect the information, criminal and civil sanctions for noncompliance imposed under the Privacy Act and other applicable federal laws, and civil rights and civil liberties protections. Census and SSS employees also take Data Stewardship Awareness training on an annual basis. Census conducts annual reviews on all data management system projects to ensure that only people authorized for the projects have access to the data.

Conclusion

In compliance with the provisions of the Privacy Act of 1974, and explicitly mandated by

[20] The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules. The title is Security Requirements for Cryptographic Modules.

Executive Order 13880, DHS is providing administrative records to the U.S. Census Bureau to assist Census in assigning a citizenship and immigration status to all persons present in the United States. Immigration status and data are notoriously difficult to combine due to its dynamic nature – individuals can have multiple immigration statuses through their lifetime. DHS has endeavored to limit the amount of information sharing with Census to promote the likelihood of linkages by Census while limiting the amount of sensitive personally identifiable information disclosed from DHS systems of record.

Responsible Officials

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services

Debbie Seguin
Chief of Staff
U.S. Customs and Border Protection

Kenneth N. Clark, Ph.D.
Assistant Director
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement

Approval Signature Page

Original, signed copy on file at the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A: U.S. Citizenship and Immigration Services Data and Project Outlines

USCIS will provide naturalization and LPR data from its Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR).[21] eCISCOR is a data repository that consolidates and manages information collected during the adjudication of applications and petitions for immigration benefits from USCIS source systems. Using the extracted eCISCOR data, USCIS will use stored logic within SAS (not an acronym)[22] to assist with data organization and aggregation. As part of this MOA, USCIS will provide an initial historical extract of records data dating back to 1973 at the end of FY 2019 and then a second extract in 2020 for data between the latest date of data provided in the first extract and April 1 2020, and as necessary and determined by DHS and the Census Bureau. The data will be transferred to the U.S. Census via a Secure File Transfer Protocol (SFTP).

Data Elements

USCIS plans to share the following data elements:

- Alien Number;
- Social Security number (SSN);
- Full Name;
- Class of admission;
- Class of admission by major category;[23]
- Whether the individual is a principal or dependent applicant;
- Date of Birth;
- Age;
- Country of birth;
- Country of last residence;
- Marital Status;
- Gender;
- Country of nationality;
- Full address;

[21] *See* DHS/USCIS/PIA-023 eCISCOR, *available at* www.dhs.gov/privacy.
[22] *See* DHS/USCIS/PIA-055 SAS Predictive Modeling Environment, *available at* www.dhs.gov/privacy.
[23] Class of Admission by major categories are the Office of Immigration Statistics yearbook of statistics categories that align with the section of law/Immigration and Nationality Act.

- Last nonimmigrant class of admission;
- Last nonimmigrant date of admission;
- Permanent Resident Card Issuance and Expiration date;
- Full U.S. residential address at the time of naturalization application;
- Date of naturalization application submission;
- Full residential address at the time of naturalization; and
- Date of naturalization.

USCIS Source Systems

As part of the MOA with Census, USCIS plans to extract the above data sets via eCISCOR:

- **Computer Linked Application Information Management System (CLAIMS 4):**[24] CLAIMS 4 is an electronic case management system used to process and adjudicate the applications associated with naturalization and/or citizenship. USCIS plans to decommission CLAIMS 4 in the near future. With the retirement of CLAIMS 4, USCIS ELIS will primarily serve as the case management system of citizenship and naturalization applications;
- **USCIS Electronic Immigration System (USCIS ELIS):**[25] USCIS ELIS serves as the internal electronic case management system for electronically filed benefit request forms and certain paper forms;
- **Central Index System (CIS 2):**[26] CIS 2 is a repository of electronic data that contains an index of basic data elements related to an individual as he or she passes through the immigration process. CIS 2 contains information on the status of applicants and petitioners seeking immigrant and non-immigrant benefits, including lawful permanent residents and naturalized citizens;
- **Reengineered Naturalization Application Casework System (RNACS):**[27] RNACS was used to process and track applications associated with naturalization and/or citizenship. RNACS has been decommissioned. eCISCOR acts as a data repository for the decommissioned data.

[24] *See* DHS/USCIS/PIA-015 Computer Linked Application Information Management System (CLAIMS 4) and subsequent updates, *available at* www.dhs.gov/privacy.
[25] *See* DHS/USCIS/PIA-056 USCIS ELIS and associated updates, *available at* www.dhs.gov/privacy.
[26] *See* DHS/USCIS/PIA-009 Central Index System (CIS) and associated updates, *available at* www.dhs.gov/privacy.
[27] *See* DHS/USCIS/PIA-023 eCISCOR, *available at* www.dhs.gov/privacy.

- **CLAIMS 3:** USCIS uses the Computer Linked Application Information Management System (CLAIMS 3) and associated systems to manage the adjudication process for most domestically-filed immigration benefit filings with the exception of naturalization, intercountry adoption, and certain requests for asylum and refugee status.
- **GLOBAL:** Global serves as the primary IT case management system for the administration of affirmative asylum, Nicaraguan Adjustment and Central American Relief Act (NACARA) § 203, withholding of removal under the terms of a settlement agreement reached in a class action, credible fear, and reasonable fear cases.

Applicable SORNs

The following Privacy Act System of Records Notices apply to the collection, use, maintenance, and dissemination of information:

- Alien File, Index, and National File Tracking System,[28] which covers the collection, use, and maintenance of benefit requests forms and supplemental information;
- Benefits Information System,[29] which covers the collection and use of immigrant and nonimmigrant benefit request forms, decisional data, and associated fees for adjudication;
- Asylum Information and Pre-Screening System of Records,[30] which covers the collection and use of affirmative asylum applications, applications filed with USCIS for suspension of deportation, special rule cancellation of removal pursuant to the Nicaraguan Adjustment and Central American Relief Act, credible fear screening cases, and reasonable fear screening cases; and,
- Refugee Case Processing and Security Information System of Records,[31] which covers the collection and use of refugee follow to join request forms, decisional data, and associated information for adjudication.

Special Protected Classes:

USCIS will share refugee and asylee data with the Census Bureau. Pursuant to 8 C.F.R. 208.6(a), the Secretary of Homeland Security must sign a waiver allowing the disclosure of refugee and asylum data to the Census Bureau. With limited exceptions, 8 C.F.R. 208.6 prohibits the

[28] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[29] *See* DHS/USCIS-007 Benefits Information System 84 FR 54622 (Oct. 10, 2019).
[30] *See* DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, 80 FR 74781 (Nov. 30, 2015).
[31] *See* DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, 81 FR 72075 (Oct. 19, 2016).

disclosure of information contained in, or pertaining to, asylum applications, credible fear determinations, reasonable fear determinations, and requests for withholding of removal. As a matter of policy, refugee applications are treated in the same manner. The purpose of this prohibition is to safeguard information that, if disclosed publicly, could subject the claimant to retaliatory measures by government authorities or non-state actors in the event the claimant is repatriated, or endanger the security of the claimant's family members of associates who may still be residing in the country of origin. Additionally, in some circumstances, public disclosure of asylum or refugee-related information might give rise to a plausible protection claim where one would not otherwise exist. The regulation, however, permits the release of such information at the discretion of the Secretary.[32] USCIS sought and is awaiting Secretarial approval to provide refugee and asylee data to Census in a Secretarial Waiver entitled, "Disclosure of Asylum Related Information to the Census." Asylum and Refugee related data will not be provided to Census until the Waiver is signed.

8 U.S.C. § 1367 generally prohibits Department personnel from permitting use or disclosure of any information relating to a beneficiary of a pending or approved application for alien victim-based immigration benefits (individuals who applied for and/or received T nonimmigrant status (victims of trafficking), U nonimmigrant status (certain victims of criminal activity), or benefits under the Violence Against Women Act to anyone other than a sworn officer or employee of DHS, the Department of State, or the Department of Justice, unless one of several enumerated statutory exceptions apply. As part of this MOA, USCIS will not disclose data related to those afforded protected status under 8 U.S.C. § 1367. USCIS and CBP apply flags to records associated with individuals afforded 1367 protections to ensure that no 1367 data is transferred to Census during the extraction process.

[32] By operation of section 1512(d) of the Homeland Security Act of 2002, the Attorney General's authority under 8 C.F.R. 208.6(a) to authorize disclosure of confidential asylum information held by the former United States Immigration and Naturalization Service – and now held by DHS –was transferred to the Secretary of Homeland Security.

Appendix B:

U.S. Customs and Border Protection Data

CBP will use the ADIS system to provide both CBP and ICE data elements, not otherwise protected from disclosure, to the Census Bureau. The business requirements and ICE data elements are identified in this PIA under Appendix C, and the use and sharing of the ICE data set will be conducted in accordance with that Appendix. Using the ADIS filtering algorithms, CBP will provide the following data elements for (1) In-Country Overstays and (2) non-immigrants lawfully in the United States within the terms of their admission.

Nonimmigrant Classes of Admission

Nonimmigrants are foreign nationals admitted temporarily to the United States within classes of admission that are defined in section 101(a)(15) of the Immigration and Nationality Act (INA). Examples of nonimmigrant classes of admission include foreign government officials, temporary visitors for business and pleasure, aliens in transit, treaty traders and investors, academic and vocational students, temporary workers, exchange visitors, athletes and entertainers, victims of certain crimes, and certain family members of U.S. citizens and lawful permanent residents (LPRs). Unlike people granted lawful permanent residency, or "green card" status, who may live in the United States with limited restrictions, nonimmigrants are authorized to enter the country for specific purposes only. Nonimmigrants' duration of stay and lawful activities, such as employment, travel, and accompaniment by dependents, are prescribed by their class of admission.

CBP will **not** provide any records regarding records tagged as protected by 8 U.S.C. § 1367.

1. **Date Range of Records**: Extract covering January 1, 2013 – December 31, 2018 to align with the 5-year American Community Survey for testing purposes. Extract covering January 1, 2019 – June 30, 2020 to align with 2020 Census respondents.
2. **Source Data System**: Arrival and Departure Information System (ADIS)
3. **System of Records Notice(s)**: DHS/CBP-021 Arrival and Departure Information System (ADIS).[33] ADIS includes aliens who have applied for entry, entered, or departed from the United States at any time. Although this system primarily consists of records pertaining

[33] DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (Nov. 18, 2015).

to alien immigrants (including lawful permanent residents) and nonimmigrants, some of these individuals may change status and become United States citizens.

4. **Individual Data Elements**, all sourced from the ADIS system:
   - Full name
   - Date of Birth (DOB)
   - Destination Address Related Data Fields (Line 1, Line 2, City, State, Zip code if available)
   - Admit Until Date
   - Passport/Visa Information
   - Gender
   - Email address
   - Telephone number
   - Social Security number (SSN) (Document Number)
   - Citizenship (at time of event as well as naturalization, if any)
   - Nationality (Document Country of Issuance)
   - Country of citizenship
   - Alien Registration Number (A-Number)
   - Event Date: Arrival Date (Departure Date)
   - Event Date: Arrival Date (Departure Date)
   - Event Type: Departure, Arrival
   - Class of admission (the following list of admission classes for Arrival Data:)
     - A3 – Attendants, servants, or personal employees of A1 and A2 and their families.[34]
     - B1 – Temporary visitors for business.
     - B2 – Temporary visitors for pleasure.
     - CW1 – CNMI-only transitional workers
     - CW2 – Spouses and children of CW1
     - E1 – Treaty traders and their spouses and children
     - E2 – Treaty investors and their spouses and children

- E2C – Treaty investors and their spouses and children (CNMI only)
- E3 – Australian Free Trade Agreement principals, spouses and children
- E3D – Spouse or Child of E3
- F1 – Academic students
- F2 – Spouses and children of F1
- M1 – Vocational students
- M2 – Spouses and children of M1
- G5 – Attendants, servants, or personal employees of representatives[35]
- H1B – Temporary workers in specialty occupations
- H1B1 – Chile and Singapore Free Trade Agreement aliens
- H1C – Registered nurses participating in the Nursing Relief for Disadvantaged Areas
- H2A – Agricultural workers
- H2B – Nonagricultural workers
- H2R – Returning H2B workers
- H3 – Trainees
- H4 – Spouses and children of H1, H2, or H3
- K1 – Fiancé(e)s of U.S. citizens
- K2 – Children of K1
- K3 – Spouses of U.S. citizens, visa pending
- K4 – Children of U.S. citizens, visa pending
- L1A and L1B – Intracompany transferees
- L2 – Spouses and children of L1
- NATO7 – Attendant, Servant, or Personal Employee of NATO1, NATO2, NATO 3, NATO4, NATO5, and NATO6 Classes, or Immediate Family
- N8 – Parent of an Alien Classified SK3 or SN3[36]
- N9 – Child of N8 or of SK1, SK2, SK4, SN1, SN2 or SN4
- O1 – Workers with extraordinary ability or achievement

- O2 – Workers accompanying and assisting in performance of O1 workers
- O3 – Spouses and children of O1 and O2
- P1 – Internationally recognized athletes or entertainers
- P2 – Artists or entertainers in reciprocal exchange programs
- P3 – Artists or entertainers in culturally unique programs
- P4 – Spouses and children of P1, P2, or P3
- Q1 – Workers in international cultural exchange programs
- R1 – Workers in religious occupations
- R2 – Spouses and children of R1
- TN – North American Free Trade Agreement (NAFTA) professional workers
- TD – Spouses and children of TN
- V1 – Spouses of permanent residents, visa pending
- V2 – Children of permanent residents, visa pending
- V3 – Dependents of V1 or V2, visa pending
- WB – Visa Waiver Program – temporary visitors for business
- WT – Visa Waiver Program – temporary visitors for pleasure

[35] Representatives refers to the other "G" classes of admission: principals of recognized foreign governments; other representatives of recognized foreign governments; representatives of non-recognized or nonmember foreign governments.
[36] *See* "Nonimmigrant Classes of Admission" for a detailed description of all codes, *available at* https://www.dhs.gov/immigration-statistics/nonimmigrant/NonimmigrantCOA#.

Appendix C:

U.S. Immigration and Customs Enforcement Data

U.S. Immigration and Customs Enforcement (ICE) operates the Student and Exchange Visitor Program (SEVP) under the authority of 8 U.S.C. § 1372, and is required to develop and manage a program to electronically collect, from approved educational institutions and designated exchange visitor programs in the United States, certain information about aliens who have or are applying for F or M nonimmigrant status.

This Appendix has been added to this PIA only to account for the transfer of ICE data elements by CBP using ADIS as noted in Appendix B. All responsive SEVP data points requested by the Census Bureau are also maintained in the CBP ADIS system. Therefore, CBP will facilitate the exchange of certain specifically identified ICE Student and Exchange Visitor Information System (SEVIS) data points within the ADIS data extract for Census according to the following ICE business requirements:

- CBP will provide an extract covering January 1, 2013 to December 31, 2018 to align with the 5-year American Community Survey for testing purposes. Extract covering January 1, 2019 to June 30, 2020 to align with 2020 Census respondents.
- CBP will provide the last ZIP Code, if available, extracted from SEVIS records as related to the address data field identified below.

As stated above, CBP will **not** provide any records regarding records tagged as protected by 8 U.S.C. § 1367 for the following ICE SEVIS data elements:

- Full name
- Date of Birth (DOB)
- Country Code
- SEVIS Active Status Data
- Active Records
- Class of admission for F and M nonimmigrants
- Mailing Address Related Data Fields (Line 1, Line 2, City, State, Zip code if available)
- Physical Address Related Data Fields (Line 1, Line 2, City, State, Zip code if available)
- Gender
- Email Address
- Telephone Number

- Visa Issue Date
- Visa Expiration Date
- Type of Visa
- Student Left Country
- Program Start Date
- Program End Date