Privacy Compliance Review of the U.S. Citizenship and Immigration Services Customer Profile Management Service & National Appointment Scheduling System

October 11, 2017

Contact Point

Donald K. Hawkins
Privacy Officer
Office of Privacy
U.S. Citizenship and Immigration Services
(202) 272-8404

Reviewing Official

Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

I. Background

The Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) oversees lawful immigration to the United States. As part of this mission, USCIS receives and adjudicates requests for immigration and citizenship benefits. The administration of these benefits requires the collection of biographic and biometric information from benefits requestors.

USCIS uses multiple systems to administer immigration benefits, including the Customer Profile Management Service (CPMS) and National Appointment Scheduling System (NASS).

- ***CPMS*** is the central USCIS repository of benefit requestors' biographic and biometric data.
- ***NASS*** is used to schedule USCIS appointments, including appointments for biometric collections at Application Support Centers (ASC).

Due to the heightened privacy risks associated with the collection of biometrics information, Privacy Impact Assessments (PIA) were completed for CPMS[1] and NASS[2] in 2015. These PIAs noted that the DHS Privacy Office (PRIV) would initiate a Privacy Compliance Review (PCR) on the ASC biometrics collection, storage, and sharing process; CPMS; NASS; and, when relevant and appropriate, the Automated Biometric Identification System (IDENT),[3] within six months of the PIA's publication in December 2015.[4]

USCIS captures biometric and related biographic data from benefit requestors to facilitate three key operational functions: (1) conduct name and fingerprint-based background checks against external systems; (2) verify benefit requestors' identity; and (3) produce benefit cards and documents.[5] Biometric information is used to conduct the required criminal background checks during the USCIS immigration benefits determination.[6]

The collection of biometrics and related biographic data is performed at authorized capture sites. Authorized capture sites include ASCs, USCIS district or field offices, and U.S. consular offices

---

[1] DHS/USCIS/PIA-060 Privacy Impact Assessment for the Customer Profile Management Service (December 17, 2015), *available at* https://www.dhs.gov/publication/dhsuscispia-060-customer-profile-management-service-cpms.
[2] DHS/USCIS/PIA-057 Privacy Impact Assessment for the National Appointment Scheduling System (July 28, 2015), *available at* https://www.dhs.gov/publication/dhsuscispia-057-national-appointment-scheduling-system.
[3] DHS/NPPD/PIA-002 Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident, and DHS/USVISIT-004 System of Records Notice for the DHS Automated Biometric Identification System (IDENT) (June 5, 2007), *available at* https://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2781.htm.
[4] CPMS PIA, *supra* note 1, at 8; *see also* NASS PIA, *supra* note 2, at 4 ("The DHS Privacy Office will initiate a Privacy Compliance Review on the ASC process, including NASS, within a year of [July 2015]").
[5] CPMS PIA, *supra* note 1, at 1.
[6] *Id.*

and military installations abroad.[7] ASCs also provide visa-related biometrics collection on behalf of the United Kingdom and of Canada.[8]

If biometrics information is required, NASS will query ASC encounter data in CPMS Query to determine whether fingerprints and/or photographs of applicants exist on file and are up-to-date in CPMS.[9] If CPMS does not already have the biometrics data on file, or if the information is out-of-date, NASS will automatically schedule an appointment by prompting the Notice Generation System (NGS) to create an appointment notice for a benefits requestor.[10] The NGS-generated appointment notice contains information for the individual (e.g., appointment location, date, and time), and information to help ASC personnel process the individual when s/he arrives (applicant name, Social Security number, date of birth, etc.).[11] Appointment confirmation letters generated by the NASS-powered InfoPass appointment scheduling service contain similar information.[12]

An individual's identity is verified when interacting with USCIS. The accuracy of the identity match depends upon the systems or processes employed. For example, when individuals appear for biometrics collection at an ASC, ASC personnel verify pre-collection that the name connected to the biometric collected matches the name on the presented form of identification.

By contrast, when individuals appear at a district or field office, USCIS personnel use the CPMS Identity Verification Tool (IVT) to "capture and submit biographic and biometric data to IDENT in order to verify an individual's established identity."[13] IDENT is the central DHS-wide system for storing and processing biometrics and associated information for identity verification purposes.[14] The biometric sample collected by CPMS IVT is then compared against the IDENT database to verify whether the information provided matches information collected during previous encounters.[15] ASCs do not currently use CPMS IVT for identity verification, but may in the future.[16]

---

[7] *Id.* at 2.
[8] DHS/USCIS/PIA-048(a) USCIS International Biometric Processing Services (November 12, 2015), *available at* https://www.dhs.gov/publication/dhsuscispia-048-uscis-international-visa-project.
[9] CPMS PIA, *supra* note 1, at 2.
[10] NASS PIA, *supra* note 2, at 1.
[11] *Id.* at 4.
[12] InfoPass (*available at* https://my.uscis.gov/appointment) is a public-facing interface that allows members of the public to schedule appointments with USCIS through the myUSCIS online portal; InfoPass was previously a standalone system, but has been integrated with NASS to create a single USCIS schedule management platform. DHS/USCIS/PIA-064 Privacy Impact Assessment for myUSCIS (December 14, 2016), *available at* https://www.dhs.gov/publication/dhsuscispia-064-myuscis.
[13] IDENT PIA, *supra* note 2.
[14] *Id.* at 1.
[15] CPMS PIA, *supra* note 1, at 2-4; *accord* IDENT PIA, *supra* note 7, at 2, 4.
[16] ASC Site Visit (April 2017).

Collected biometrics and related biographic data are stored locally on the biometrics workstation and submitted through the Enterprise Service Bus (ESB) to CPMS Query.[17] CPMS may then send queries of the collected data via ESB to IDENT, the FBI Central Records System (CRS), Universal Index (UNI), the Next Generation Identification (NGI) system, or the DoD Automated Biometric Identification System (ABIS)[18] in order to conduct the requisite background checks.[19] CPMS may also send biometrics and biographic data to other USCIS systems for the production of benefit cards and documents. For example, CPMS sends relevant information to the Integrated Card Production System (ICPS) and Travel Document Processing System (TDPS) for applications processed by the Computer Linked Application Information Management System 3 (CLAIMS 3).[20]

II. Scope and Methodology

Scope

The scope of this PCR will focus on the collection, use, and dissemination of biometric information within CPMS, NASS, and IDENT as defined in privacy compliance documents, as well as standard operating procedures (SOP) at ASCs. Given the expansive nature of this PCR, the findings in this PCR report do not exhaustively review every FIPP for all systems. While PRIV endeavors for all PCR reports to reflect the current state of reviewed system, the scope of this report is limited to reviewing the issues highlighted by existing privacy compliance documentation and any critical compliance issues discovered in the course of this PCR. Furthermore, as evidence of the collaborative format that the PCR process allows, USCIS proactively implemented PRIV's suggested modifications to ASC SOPs that were revealed during the course of our review.

Methodology

The PCR is a collaborative process that ensures programs operate in compliance with federal privacy laws, departmental policies, and assurances made in PIAs, System of Records Notices (SORN), and other privacy compliance documentation. This PCR was conducted in coordination with USCIS system and program managers, USCIS subject matter experts, and the USCIS Privacy Office. This report will organize our review according to the DHS Fair Information Practice Principles (FIPPs) framework.[21]

In conducting this PCR, the DHS Privacy Office:

- Reviewed CPMS, NASS, IDENT, and other relevant PIAs;

[17] CPMS PIA, *supra* note 1, at 2.
[18] Privacy Impact Assessment for the Department of Defense Automated Biometric Identification System (DoD ABIS) (November 2008), *available at* http://ciog6.army.mil/PrivacyImpactAssessments/tabid/71/Default.aspx (located under "ABIS"; direct link to PIA: http://ciog6.army.mil/Portals/1/PrivacyImpactAssessments/2015/DoD%20ABIS.pdf).
[19] CPMS PIA, *supra* note 1, at 5-6.
[20] *Id.* at 6.
[21] DHS Policy Directive 140-06 (Privacy Policy Guidance Memorandum 2008-01) "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security" (December 29, 2008), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

- Reviewed relevant SORNs;
- Developed initial questionnaire (September 2016);
- Held introductory site visit and discussion at USCIS Privacy Office (September 2016);
- Reviewed initial USCIS responses and supporting documentation;
- Developed follow-up questionnaires (November 2016, January 2017, February 2017);
- Reviewed follow-up USCIS responses and supporting documentation;
- Held a follow-up site visit and discussion at USCIS Privacy Office (January 2017);
- Held a site visit at a USCIS ASC (Glenmont, MD) to observe biometrics collection processes (April 2017);
- Drafted an initial PCR Report (August 2017);
- Adjudicated USCIS comments (September 2017);
- Drafted and published final PCR Report.

III. Findings

A. Summary of Recommendations

The DHS Privacy Office notes USCIS compliance with privacy requirements of federal privacy laws, DHS and Component privacy regulations and policies, and explicit assurances made by USCIS in existing privacy compliance documentation. Furthermore, USCIS engages in best practices throughout CPMS, NASS, and other associated systems and information collection processes. These best practices in particular should be held up as a model for other USCIS and DHS programs and systems. Based on our findings, the DHS Privacy Office makes the following recommendations:

1. USCIS should ensure that all forms of public notice accurately and consistently reflect how information is currently collected, used, disseminated, or maintained by the system in question;
2. As a best practice, USCIS should consider providing additional information at the point of collection, especially when consent is implied through an individual's conduct in lieu of express written consent;
3. As a best practice, instead of articulating authorities merely by citing to a statute or regulation, USCIS should consider explaining what is authorized by the cited legal authority;
4. USCIS should consider implementing a retention period for locally stored temporary records in a future update to the ASC workstation software;
5. USCIS should finalize a NARA-approved retention schedule for NASS if it has not already done so; and
6. As a best practice, USCIS should consider the feasibility of implementing multi-layered encryption for other "at rest" data.

Note: recommendations that begin with "USCIS should …" are recommendations that must be implemented to bring USCIS into compliance with existing federal privacy laws, DHS and

Component privacy regulations and policies, including the DHS FIPPs, or explicit assurances previously made by USCIS in privacy compliance documentation.

Recommendations that begin with "As a best practice …" highlight the best practices USCIS has already implemented in limited circumstances and encourages USCIS to consider adopting these practices more broadly, as appropriate, to further enhance USCIS's privacy posture. Best practice recommendations are not required as USCIS has already met the threshold standard of privacy compliance.

B. Transparency

DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).[22]

Finding: USCIS generally provides sufficient notice, but should ensure information contained in the notice is consistent.

USCIS provides notice to immigration benefit requestors regarding the collection, use, dissemination, and maintenance of PII in PIAs,[23] SORNs, and in notices that meet section 552a(e)(3) requirements of the Privacy Act (privacy notices), including application form instructions.[24] This PCR will focus on privacy notices as individuals are most likely to encounter these types of notice during or immediately prior to the collection of PII.

Privacy notices describe: 1) the system's legal authority for collecting the information; 2) the purpose(s) for collecting the information and how DHS will use it; 3) whether providing the information is mandatory or voluntary; and 4) to whom DHS may disclose the information and for what purpose(s).[25] Even when not required by the Privacy Act or other legal obligations, DHS endeavors to include privacy notices on all information collections.[26] For example, the InfoPass privacy notice 1) cites to 8 U.S.C. 1100 et seq.; 2) explains that the collected information will be used to schedule appointments; 3) explains that this information collection is voluntary (noting the appointment may not be successfully scheduled if information is not provided); and 4) describes all the ways in which the collected information may be used.[27]

---

[22] DHS Policy Directive 140-06 (Privacy Policy Guidance Memorandum 2008-01) "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security", at 3 (December 29, 2008), *available at* https://www.dhs.gov/publication/fair-information-practice-principles-fipps-0.
[23] *Id.*
[24] *Field v. Brown*, 610 F.2d 981, 987 (D.C. Cir. 1979) (holding that an agency's form "contained all the elements required by 5 U.S.C. § 552a(e)(3)").
[25] U.S. Department of Homeland Security Privacy Act Statement Guidance, *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_e3.pdf.
[26] DHS Privacy Policy Guidance Memorandum 2017-01 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information", at 3 (April 27, 2017), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.
[27] InfoPass privacy notice ("Privacy Act Statement"), *available at* https://my.uscis.gov/appointment.

Additional notice may be provided through form instructions at the point of collection.[28] The instructions found on the InfoPass submission form (reproduced below) are one example:

> To confirm your appointment, please enter the information requested below. We use this information only for scheduling purposes and will not share it with anyone else. We need your phone number in case we need to contact you to cancel an appointment.[29]

However, the disclosure notice provided by the InfoPass form instruction appears to contradict the notice provided by the InfoPass privacy notice. Although the InfoPass form instruction states that collected information will not be shared with anyone else, the InfoPass privacy notice informs individuals that collected information may be shared with other entities in accordance with approved routine uses. Further review by the DHS Privacy Office shows that although the NASS PIA[30] and InfoPass PIA[31] both currently state that sharing outside of DHS is not an approved routine use, NASS data may however be shared[32] with the Department of State for security clearance purposes when individuals visit USCIS international offices located in U.S. Embassies and Consulates.

The DHS Privacy Office recognizes the challenges of documenting changes across a complex web of interconnected systems, and recognizes that the supposed contradiction may have resulted from the natural frictional lag in documenting changes in ever-evolving systems or other innocuous reasons. However, as contradictory information may create confusion and erode public confidence, the DHS Privacy Office recommends that USCIS ensure that all public notice provided for any given system is accurate and consistent.

Recommendation

1. USCIS should ensure that all forms of public notice accurately and consistently reflect how information is currently collected, used, disseminated, or maintained by the system in question.

C. Individual Participation

DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should

---

[28] *See Field v. Brown*, *supra* note 24.
[29] InfoPass Appointment Scheduling Form, *available at* https://my.uscis.gov/appointment.
[30] NASS PIA, *supra* note 2, at 12, 15.
[31] DHS/USCIS/PIA-046 Privacy Impact Assessment for USCIS Customer Scheduling and Services, § 6.1 at 16 (March 25, 2014), available at https://www.dhs.gov/publication/dhsuscispia-046-customer-scheduling-and-services.
[32] Information sharing with the Department of State is addressed in DHS/USCIS/PIA-046 *available at*: https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-cssinfopass-march2014.pdf. Note the NASS PIA uses the Benefit Information System SORN (*available at*: https://www.regulations.gov/document?D=DHS_FRDOC_0001-1511) and Asylum Information and Pre-Screening (*available at*: https://www.gpo.gov/fdsys/pkg/FR-2015-11-30/html/2015-30270.htm) SORN to operate, which both include routine uses that allow for information sharing between State and USCIS to process petitions.

also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.[33]

Finding: The amount of notice given to individuals when consent is implied or explicit should correlate to the sensitivity of the collected data, and when relying on implied consent, consistent notice and access to more information should be provided to the individual throughout the process.

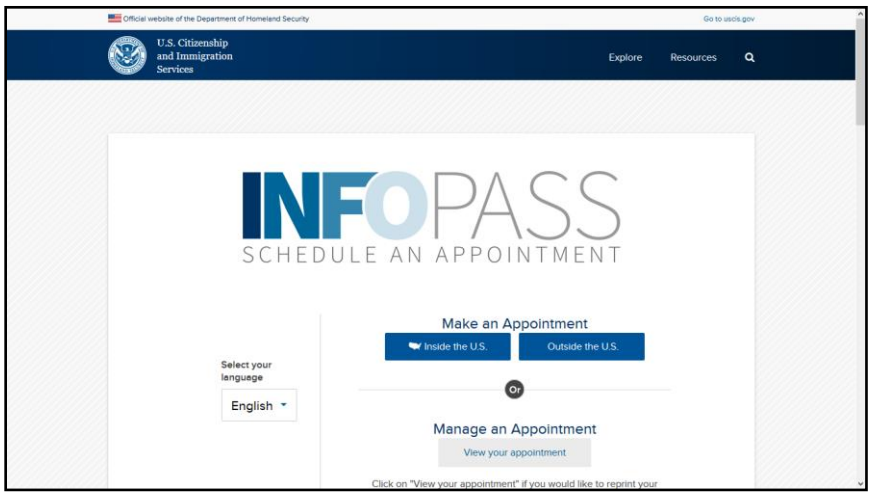
Individuals may consent to the collection, use, dissemination, and maintenance of PII either through their express consent or as implied by their conduct. For example, individuals expressly acknowledge when signing Part 7 of Form I-751, that they "understand that the purpose of a USCIS ASC appointment is for me [the individual] to provide fingerprints, photograph, and/or signature to re-affirm that all of the information in my [the individual's] petition is complete, true, and correct and was provided by me [the individual]."[34] Similarly, individuals also give their express written consent during the I-90 biometric capture process when they are asked to attest they "have reviewed and understand [the individual's] application, petition, or request I-90" with their signature.

Individuals may also be asked to give consent through "clickwrap" or "browsewrap" agreements when providing PII through a website. A "clickwrap agreement" describes a form of express consent when users must affirmatively consent to a website's terms of service by checking a box or clicking a button acknowledging agreement before they are allowed any further access. "Browsewrap agreements" are a form of implied consent in which the continued use of the website itself signals consent to the terms of service.

The NASS InfoPass interface contains elements of both clickwrap and browsewrap agreements. Like a clickwrap agreement, InfoPass users must affirmatively click a button to leave the home page and schedule an appointment. However, InfoPass is missing several clickwrap elements that would make it fully an express consent agreement: the InfoPass click-through buttons do not explicitly require an affirmative acknowledgement and agreement to the terms of service (*Figure 1*, below), nor is the user prevented from further accessing the website before making an affirmative acknowledgment. The DHS Privacy Office is not stating that the sensitivity of the information collected and used to complete the InfoPass process necessarily warrants express consent, but portions of this process reflect steps in an express consent agreement where USCIS should be recognized for implementing this as a best practice.

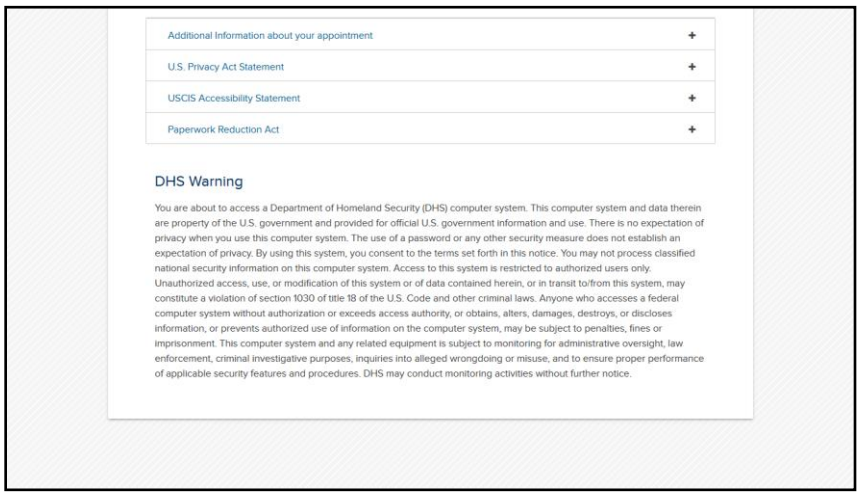
[33] DHS FIPPs, *supra* note 8, at 3.
[34] DHS USCIS Petition to Remove Conditions on Residence, Form I-751 (OMB No. 1615-0038), at 6, *available at* https://www.uscis.gov/i-751.

Figure 1: InfoPass home page



When relying on implied consent, consistent notice and access to more information should be provided to the individual throughout the process. The InfoPass application, however, does not display the terms of service consistent with best practices of browsewrap agreements. The InfoPass terms of service (the privacy notice, as made up by the "Privacy Act Statement" and "DHS Warning") are also located well below the "Make an Appointment" or "Manage an Appointment" buttons [compare the location of the scrollbar on the right side of the InfoPass homepage screenshot in Figure 1 (above) to Figure 2 (below)]. InfoPass also does not contain multiple notifications to hyperlinked terms of service throughout the appointment scheduling process. PRIV believes the InfoPass website could provide consistent and timelier information to users and therefore, USCIS should consider providing additional information throughout the information collection process.

Figure 2: InfoPass home page, Privacy Act Statement and DHS Warning



USCIS does, however, demonstrate later in the InfoPass process, more effective and timely notice via the InfoPass appointment submission form:

> To confirm your appointment, please enter the information requested below. We use this information only for scheduling purposes and will not share it with anyone else. We need your phone number in case we need to contact you to cancel an appointment.[35]

Form instructions are especially valuable as other types of notice may be overlooked. For example, the InfoPass privacy notice ("Privacy Act Statement") is located in the collapsible field (Figure 2, above). Instructions like this InfoPass example are an effective notification tool as they provide the general public with a clear and direct explanation for *why* and *when* the information is requested and should be more broadly adopted by USCIS. Individuals may also be encouraged to provide more and/or better quality information when there is a clear understanding of the collection purposes.

Finding: USCIS provides individuals multiple ways to access, correct, and redress their information.

The DHS Privacy Office found that individuals have several methods to access, correct, or redress information contained in CPMS or NASS:

- Benefit applicants are able to view their information during in-person ASC appointments.
- Corrections to typographic errors on USCIS notices, documents, or cards can be made through the USCIS online typographic error correction form.[36]
- Benefit requestors may change the name associated with their application to reflect a legal marriage, divorce, adoption, or name change petition by submitting the relevant legal documentation to USCIS for review. Individuals can also submit documentation relevant to a name change in-person during an InfoPass appointment or online through the "Other Evidence" option in their USCIS online account.[37]
- Applicants are able to view their information during an ASC biometrics processing appointment.
- Other "request[s] for change[s] in data that is not due to error" may also be corrected in-person during an InfoPass appointment.
- If a data edit in CPMS becomes necessary, a USCIS official can submit a G-1273 Data Edit request form to the USCIS Biometrics Division on behalf of a benefits requestor.[38]

---

[35] InfoPass Appointment Scheduling Form, *available at* https://my.uscis.gov/appointment.
[36] USCIS Customer Service Online Tools – Typographic Error Correction Form, *available at* https://egov.uscis.gov/e-request/displayTypoForm.do?entryPoint=init&sroPageType=typoError.
[37] USCIS Preparing for Your Biometrics Services Appointment – Requests to Change Your Name or Other Personal Information, *available at* https://www.uscis.gov/forms/forms-information/preparing-your-biometric-services-appointment#Requests.
[38] CPMS PIA, *supra* note 1, at 19; *accord* USCIS Response to PCR Questionnaire Q4.c.ii, at 3 (Dec. 28, 2016).

Individuals may also file Freedom of Information Act (FOIA) or Privacy Act Requests by mail.[39] No form is necessary to file a FOIA or Privacy Act Request. However, individuals may use the USCIS FOIA and Privacy Act Request form, Form G-639, to ensure they have included all necessary information to successfully process a FOIA or Privacy Act Request as specific information is required to respond to the Request.[40]

Recommendation

2. As a best practice, USCIS should consider providing additional notice at the point of collection, especially when consent is implied through an individual's conduct in lieu of express written consent.

D. Purpose Specification

DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.[41]

Finding: Articulations of authorities could be made clearer with explanations of the cited statues and regulations.

While the NASS articulations of authority meet the threshold requirements of the Purpose Specification FIPP, a simple legal citation may not provide much clarification to individuals unfamiliar with the cited statute or with legal citations in general. For example, the NASS PIA states, "The authority to collect information is found within the Immigration and Nationality Act (INA). [Fn 9: 8 U.S.C. §§ 1101, 1103, 1201, and 1255.]"[42] Similarly, the InfoPass privacy notice ("Privacy Act Statement") states, "The Immigration and Nationality Act, as amended, 8 U.S.C. §§ 1101, 1103, 1201, and 1255 authorizes USCIS to collect the information to schedule an appointment."[43]

Even a cursory explanation of the cited statutes would provide the general public with a greater substantive understanding of the relevant authorities. USCIS has already provided additional explanations in some instances. For example, although the CPMS PIA similarly states, "The legal authority to collect biometric and associated biographic information, including SSN, comes from 8 U.S.C. § 1101 et seq.," it goes on to explain:

> Section 103(a) of the Immigration and Nationality Act (INA) sets forth the Secretary of Homeland Security's authority to administer and enforce the immigration and naturalization laws. In particular, under section 103(a)(3) of the INA, the Secretary of Homeland Security is authorized to prescribe forms, issue instructions, and perform other acts as deemed necessary to carry out his authority under the INA. DHS regulations at 8 CFR § 103.16(a) provide that any individual may be required to submit biometric information if the regulations or form instructions

[39] CPMS PIA, at 18-19; *accord* NASS PIA, *supra* note 2, at 13.
[40] USCIS | How to File a FOIA/PA Request, *available at* https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia/how-file-foia-privacy-act-request/how-file-foiapa-request.
[41] DHS FIPPs, *supra* note 8, at 3.
[42] NASS PIA, at 4.
[43] InfoPass, *supra* note 26.

> require this information or if requested in accordance with 8 CFR § 103.2(b)(9). Also, DHS is authorized under 8 CFR § 103.16(a) to use the biometric information collected to conduct background and security checks, adjudicate immigration and naturalization benefits, and perform other functions related to administering and enforcing the immigration and naturalization laws. DHS regulations at 8 CFR § 103.2(b)(9) provide that any applicant, petition, or any other individual may be required to appear for fingerprinting or an interview. As described in 8 CFR § 103.16(a), the more specific authority to conduct background checks through fingerprint and photograph collection is identified in regulations governing the particular benefit being requested.[44]

Unlike the NASS articulations of authority, the CPMS PIA goes on to explain what information collection or use is permitted by the cited statute or regulation. As is seen here, articulation of authority or a form instruction can provide even greater transparency and clarity when paired with an articulation of purpose as they explain *why* information is being collected. This type of notice is ultimately more informative for the general public than a simple legal citation.

Recommendation

3. As a best practice, instead of articulating authorities merely by citing to a statute or regulation, USCIS should consider explaining what is authorized by the cited legal authority.

E. Data Minimization

> *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).*[45]

Finding: USCIS collection of PII is directly relevant and necessary to accomplish specified purposes.

The DHS Privacy Office confirmed that the PII collected by CPMS[46] is directly relevant and necessary to accomplish its stated purpose. Specified CPMS purposes include being the centralized repository of biometrics captured by USCIS, being the centralized authoritative source of image sets for benefit card and document production, and facilitating identity verification. For example, supplying facial images for benefits cards production requires not only the images themselves (biometrics information), but additional, biographic information associated with the applicant (individual information, demographic information) and the card data itself in order to correctly match the image to the corresponding card.

NASS collects PII from USCIS case management systems[47] and, potentially, from individuals themselves or their legal representatives.[48] Specified NASS purposes include scheduling appointments, generating appointment notices, and verifying applicant identity. The DHS

[44] CPMS PIA, *supra* note 1, at 8.
[45] DHS FIPPs, *supra* note 8, at 4.
[46] CPMS PIA, *supra* note 1, at 10.
[47] NASS PIA, *supra* note 2, at 9.
[48] *E.g.*, InfoPass, *supra* at 7.

Privacy Office finds the PII collected by NASS is directly relevant and necessary to accomplish these purposes.

NASS further minimizes PII collection by utilizing existing information in CPMS when possible and only scheduling additional biometric collection appointments if necessary. If a benefit requestor's biometric information was collected within the past five years, USCIS will use the previously collected biometric information instead of collecting the biometric information again.

Finding: ASCs have good reason to temporarily retain a locally stored copy of the collected biometric and biographic information, but should as a best practice consider setting a retention period for these temporary records.

The DHS Privacy Office conducted a site visit to observe the biometrics collection process at an ASC in Glenmont, Maryland.[49] During the site visit, PRIV observed that the biometrics workstation computer hard drive retained a record of the collected biometric and biographic information.[50] PRIV asked: 1) why does the ASC retain a record of the collected biometric and biographic information on the workstation local hard drive instead of immediately deleting the record after transmitting it to CPMS; and, 2) what was the retention period for locally-stored records?

The ASC On-Site Program Manager explained that the collected information was locally retained for a period of time as a redundancy against network connectivity issues or technical difficulties with CPMS ESB. If the workstation record was immediately deleted, the benefit applicant would have to undergo another biometrics collection appointment and incur a potential delay in the processing of his/her benefit application in the event of an unsuccessful transmission. With the workstation copy, however, the ASC would only need to resend the locally-stored information.

There is currently no set retention period for records locally stored on the workstation hard drive. Records are retained for as long as there is space on the hard drive.[51] The retention period may be a matter of days for a higher-volume ASC, and potentially weeks or perhaps months for a lower-volume ASC.[52] PRIV recognizes that addressing this issue may not be an agency priority at this time given that the length of time records are retained for many ASCs may be within a standard retention period. However, data retention is a privacy concern as the longer data are retained, the greater the risk of its misuse.

The DHS Privacy Office therefore recommends as a best practice that USCIS consider implementing a period-based retention schedule for locally stored temporary records in a future update to the ASC workstation software.

---

[49] ASC Site Visit (April 2017).
[50] *Id.*
[51] *Id.*
[52] *Id.*

Finding: USCIS retention periods correlate to the specified purposes, but a full explanation of those purposes was not initially provided.

CPMS records are retained for100 years from the individual's date of birth in accordance with NARA Disposition Authority.[53] In the CPMS PIA, USCIS states "there is a direct correlation between an Applicant's A-file" and the CPMS records retention period (Alien Files, or "A-Files," are retained for 100 years after the birth date of the file subject), because an individual may continue to interact with USCIS throughout his/her life if s/he does not become a naturalized citizen.[54]

There is no current NARA-approved retention schedule for NASS, but USCIS plans to implement a similar, 99-year retention period for NASS records because "both systems [CPMS and NASS] contain pertinent data needed for adjudication," and "because the relationship between an applicant and USCIS may span the applicant's entire life."[55] NASS records are currently retained indefinitely until a NARA-approved retention schedule is finalized and approved.[56]

The DHS Privacy Office initially questioned whether the 99-year retention period for NASS records is "necessary to fulfill the specified purposes" of the NASS system as the specified purposes of NASS are to schedule ASC (and other) appointments and generate appointment notices. A record of an appointment would appear to fulfill its specified purpose once the individual attends and subsequently concludes his or her scheduled appointment. Similarly, a record of an unattended or cancelled appointment would appear to fulfill its specified purpose once a new appointment is made or the benefits application is either withdrawn or denied—and would in any case appear to be superseded by the record of the final appointment or adjudication.

However, USCIS responded by stating records would be retained after the subject's death both because "aliens can request an immigration benefit through a deceased qualifying relative" and for genealogical purposes. Additional fact-finding conducted during this PCR found that routine administrative or clerical documents have historically been retained in immigration files and possess historical research value.[57] The DHS Privacy Office therefore finds that a 99-year retention period for NASS records is in keeping with the long-held historical use purpose of immigration records.

---

[53] CPMS PIA, *supra* note 1, at 9; *accord* NARA Disposition Authority Number DAA-0563-2013-0001-0005 *available at* https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf. *See also* NARA Disposition Authority Number DAA-0563-2013-0001-0001 "Adverse Background Screening Results", and NARA Disposition Authority Number DAA-0563-2013-0001-0002 "Favorable Background Screening Results."

[54] CPMS PIA, *supra* note 1, at 15.

[55] NASS PIA, *supra* note 2, at 5.

[56] *Id.* at 11.

[57] *E.g.*, USCIS | History and Genealogy | A-Files' Research Value https://www.uscis.gov/history-and-genealogy/genealogy/files-numbered-below-8-million#ResearchValue; *accord* USCIS | History and Genealogy | A-Files Image Gallery, *available at* https://www.uscis.gov/history-and-genealogy/genealogy/files-image-gallery.

Recommendations

4. USCIS should consider implementing a retention period for locally-stored temporary records in a future update to the ASC workstation software.
5. USCIS should finalize a NARA-approved retention schedule for NASS if it has not already done so.

F. Use Limitation

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.[58]

Finding: CPMS and NASS mitigation measures reduce the risk that PII is used outside of specified purposes.

The CPMS PIA identified the following mitigation measures:

1. All users are required to sign a CPMS- or Person Centric Query Service (PCQS)-specific Rules of Behavior indicating that they have read, understand, and agree to abide by the system policies, before the supervisor and Accounts Management Branch authorizes access to information and the information system;
2. Only users who have a need to know the information in the system can gain access to CPMS, and that access is restricted to what is necessary to perform specific job-related functions;
3. Users receive training on how to use CPMS and the restrictions on sharing the information it contains;
4. All users' actions are recorded and periodically audited by program management;
5. Users have all been informed that inappropriate use of the system or information contained therein could lead to reprimands and job loss; and
6. All users also receive training on the proper handling of information in accordance with laws, regulations, and policy, including but not limited to the Privacy Act.[59]

Mitigation measure 2 will be discussed as part of § III.H. Security, below; mitigation measures 3, 4, and 6 will be discussed as part of § III.I. Accountability and Auditing, below.

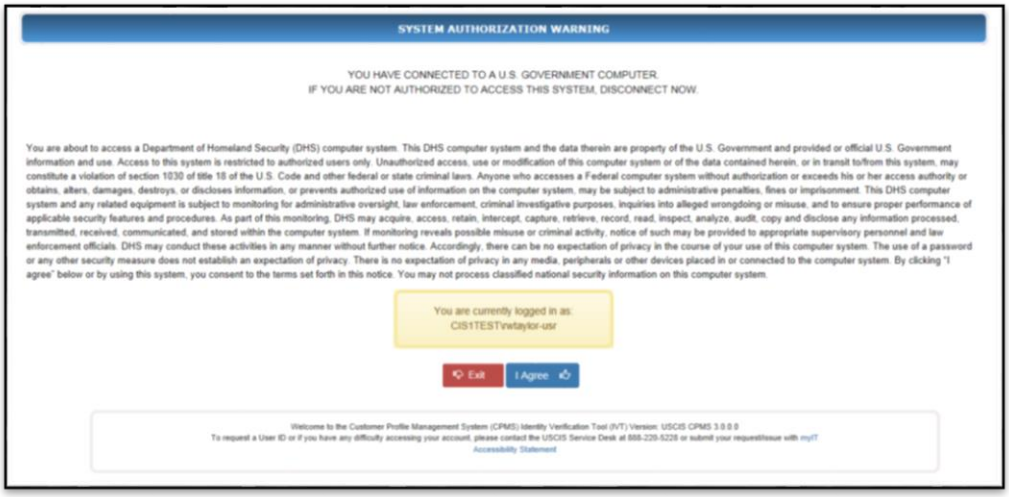
Mitigation measure 1 states that all users must sign a CPMS- or PCQS-specific Rules of Behavior before they are authorized access to CPMS. The USCIS Privacy Office provided examples of both the USCIS General Rules of Behavior and the USCIS ESB Rules of Behavior. The USCIS ESB Rules of Behavior govern the behavior of "ESB end users as well as for the systems being connected by the ESB," which include CPMS.[60] The rules of behavior describe

[58] DHS FIPPs, *supra* note 8, at 4
[59] CPMS PIA, *supra* note 1, at 13.
[60] USCIS Enterprise Service Bus System Rules of Behavior.

system access, access control, data protection, incident reporting, accountability, and other miscellaneous rules, as well as the consequences of non-compliance.[61]

Mitigation measure 5 states that users have all been informed that inappropriate use of the system or information contained therein could lead to reprimands and job loss. As the screenshot of the CPMS-IVT System Authorization Warning Screen (*Figure 3*, below) shows, users are informed that "anyone who accesses a Federal computer system without authorization or exceeds his or her access authority or obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on the computer system, may be subject to administrative penalties, fines, or imprisonment."

Figure 3: CPMS-IVT System Authorization Warning Screen



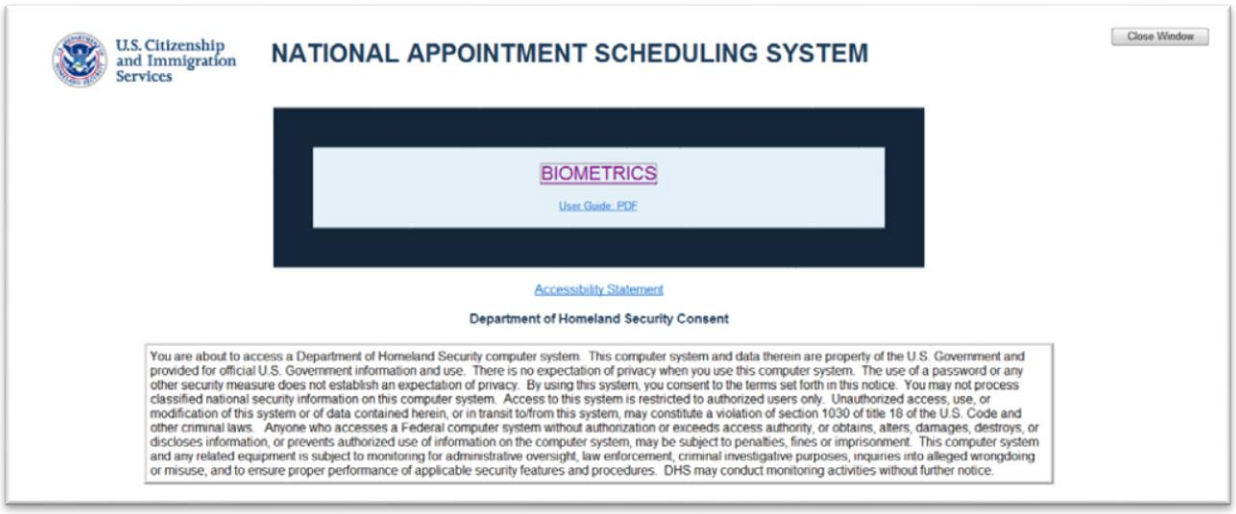
The NASS PIA identified the following use of PII mitigation measures:

1. A warning banner on the log-in screen informs users that the system may be monitored to detect improper use, and the consequences of illicit use of the data;
2. The system's auditing capability records users' activities in the system; and
3. The system's audit logs are reviewed on a regular basis by system administrators to ensure that the system is being used appropriately.[62]

Mitigation measure 1 describes the notice provided by the log-in screen. As the screenshot of the NASS homepage (*Figure 4*, below) shows, the NASS log-in screen informs users that their use of NASS may be monitored, and "unauthorized access, use, or modification of this system or of data contained herein, or in transit to/from this system, may constitute a violation of section 1030 of title 18 of the U.S. Code and other criminal laws."

[61] *Id.*
[62] NASS PIA, *supra* note 2, at 10.

Figure 4: NASS Homepage



Finding: Information sharing purposes are compatible with the collection purpose.

CPMS information may be shared with the Department of State, under Routine Use C of the DHS/USCIS-003 Biometric Storage System SORN, for visa and passport adjudication responsibilities, as well as fraud detection and investigation responsibilities.[63] This information sharing is compatible with the CPMS purpose of collecting information to process petitions or applications for immigration-related benefits under the Immigration and Nationality Act.

CPMS information may be shared with the Department of Justice and the Department of Defense, under Routine Use G of the DHS/USCIS-002 Biometric Check System SORN, to verify through name and fingerprint checks that an applicant is eligible for the immigrant benefit being sought.[64] CPMS also shares biometric and limited biographic information within DHS with IDENT during the identity verification process. These information sharing arrangements are compatible with the CPMS purpose of collecting information for identity verification.

Although current NASS documentation states that NASS information will not be shared outside of DHS,[65] a forthcoming PIA update will describe how NASS information is shared with the Department of State to verify the identity of visitors to USCIS International Offices located in U.S. Embassies and Consulates. (*See* § III.B. Transparency, *above*.) As identity verification is also a purpose of the initial collection, this is an approved routine use of that information.

---

[63] Biometric Storage System of Records Notice, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2007-04-06/html/07-1643.htm.
[64] Background Check Services System of Records Notice, *available at*: https://www.gpo.gov/fdsys/pkg/FR-2007-06-05/html/07-2782.htm. .
[65] NASS PIA, at 12.

Recommendation

- No recommendations.

G. Data Quality and Integrity

DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.[66]

There is little indication that the quality and integrity of data collected by CPMS or NASS are an issue. All parties to the data collection have substantial interests in insuring any and all collected PII is accurate, relevant, timely, and complete.

Furthermore, CPMS and NASS contain multiple checkpoints throughout the collection process to ensure data and integrity. The multiple rounds of review and adjudication that make up the immigration benefits application process allow both parties opportunities to identify any instances of inaccurate data. For instance, some applicants may refuse to sign Attestation Language because the information shown during the ASC biometrics collection does not reflect information they believe to be true. In these circumstances, the ASC SOP therefore instructs the ASC-ISO to review that applicant's USCIS records to mitigate the issue.

Within NASS, a separate series of data integrity checks ensure proper vetting, identity matching, and records formatting: a receipt check determines whether a particular schedule request has been processed; a second check determines whether the biometrics associated with that particular request already exist in CPMS and whether it has been collected within the past five years; and a fingerprint background check determines whether such a check has already been completed for the benefit requestor.

Recommendation

- No recommendations.

H. Security

DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.[67]

Note: The scope of this PCR primarily focused on the security controls explicitly described as a privacy mitigation measure (*see* § III.F. Use Limitation, *above*).

Finding: User Access Controls were designed to restrict access to USCIS systems.

Approximately 4,000 internal users across DHS—including the U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP), and the DHS Office of

[66] DHS FIPPs, *supra* note 8, at 4
[67] DHS FIPPs, *supra* note 8, at 4

Biometric Identity Management (OBIM)—and external users at the Department of State have access to CPMS. A large user base with access to sensitive PII presents an inherent security risk.

This type of risk may be mitigated with strict user access controls. CPMS use of PII mitigation measure 2 states, "Only users who have a need to know the information in the system can gain access to CPMS, and their access to information contained within the system is restricted to what is necessary to perform specific job-related functions."

USCIS role-based access controls allow supervisors to assign specific users different levels of access to CPMS privileges as specified by users' respective roles. CPMS users are only granted the minimal level of access required to complete their respective duties. For example, CPMS general users only have query access to view and print biometric data, which limits the possibility of improper use of PII. As an added precaution, employees seeking Administrator-level access must also receive approval from USCIS's Biometrics Division.

CPMS users' interactions with the system are also tracked through audit logging (*see also* § III.I. Accountability and Auditing, *below*).

Finding: The multi-level encryption protocol recently implemented to protect CPMS data "at rest" provides a significant level of protection, and may be appropriate for further implementation.

There is an inherent risk that bad actors may gain access to information stored in or transferred between electronic systems. USCIS mitigates this risk by encrypting data to deny access to the information even if the transmission was intercepted. Data "at rest", when data are not moving in between networks or systems, is generally stored in an unencrypted format as the risk of loss is generally lower. However, the risk is still non-zero, and the sensitivity of the database in question may make it appropriate to provide additional safeguards to "at rest" data.

With that in mind, USCIS has recently implemented multi-layered encryption for CPMS "at rest" data. This multi-layer approach provides a significant additional level of security for "at rest" data and all parties involved in implementing this project are right to be proud of the success of this initiative. The DHS Privacy Office commends USCIS for the success of this first initiative, and encourages USCIS to consider implementing multi-layered encryption (or other security controls) for other categories of "at rest" data as appropriate.

Recommendation

6. As a best practice, USCIS should consider the feasibility of implementing multi-layered encryption for other "at rest" data.

I. Accountability and Auditing

DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[68]

Finding: USCIS has demonstrated compliance with the Accountability and Auditing FIPP.

The DHS Privacy Office evaluated whether USCIS provided adequate training for their employees and contractors who use PII, and whether USCIS has sufficiently audited the actual use of PII.

The DHS Privacy Office finds the training provided by USCIS to be adequate. The PCR evaluated the adequacy of training materials by comparing them with compliance documentation and other reference materials. Compliance documentation and other such materials describe how systems should be operated in accordance with applicable privacy protection requirements. Training materials may thus be deemed adequate when they instruct a new user to act in accordance with compliance documentation; training materials that significantly depart from documentation are not.

The DHS Privacy Office also finds that USCIS has adequately audited the actual use of PII. The CPMS and NASS PIAs describe three mitigation measures related to auditing: according to CPMS mitigation measure 4, "All users' actions are recorded and periodically audited by program management;" NASS mitigation measures 2 states "The system's auditing capability records users' activities in the system;" and NASS mitigation measure 3 guarantees, "The system's audit logs are reviewed on a regular basis by system administrators to ensure that the system is being used appropriately." (*See* § F. Use Limitation, above.)

CPMS and NASS are regularly audited by the Office of the Chief Information Officer (OCIO) as part of the USCIS Continuous Diagnostics and Mitigation (CDM) Ongoing Authorization (OA) Program. The USCIS OA Program replaces the traditional Authority to Operate (ATO) model; instead of undergoing a full Security Control Assessment (SCA) once every three years, USCIS OA Program systems are continually monitored, audited, and evaluated for security risks.

Although the traditional SCA model allows the DHS Privacy Office greater oversight of privacy controls than what is currently provided through the OA Program, the DHS Privacy Office has found no evidence during this PCR that OA Program controls are insufficient. This finding is supported by the DHS Office of Inspector General (OIG) report, "Evaluation of DHS' Information Security Program for Fiscal Year 2016," which found that USCIS training and audit control measures either met or exceeded Department expectations.[69]

---

[68] DHS FIPPs, *supra* note 8, at 4
[69] DHS OIG 17-24, Evaluation of DHS' Information Security Program for Fiscal Year 2016, 31 (January 18, 2017), *available at* https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-24-Jan17.pdf.

Recommendation

- No recommendations.

IV. Conclusion

The DHS Privacy Office would like to commend USCIS for not only complying with privacy requirements of federal privacy laws, DHS and Component privacy regulations and policies, and explicit assurances made by USCIS in prior privacy compliance documentation, generally, but for engaging in best practices throughout CPMS, NASS, and other associated systems and information collection processes. These best practices in particular should be held up as a model for other USCIS and DHS programs and systems.

This PCR includes recommendations addressing areas in which USCIS could further enhance their privacy posture. The DHS Privacy Office also strongly encourages that USCIS consider implementing best practices recommendations as appropriate. To that end, the DHS Privacy Office requests that the USCIS Privacy Office:

- monitor the implementation of this PCR's recommendations and update, as needed, relevant CPMS, NASS, or other privacy compliance documentation to reflect the findings and/or outcomes of this PCR; and
- provide a written report on the implementation status of all recommendations within 12 months of this PCR's publication date. For any recommendations that USCIS has not implemented or has chosen not to implement in that timeframe, including best practice recommendations, PRIV requests that USCIS explain why the recommendations were not implemented.

Finally, the DHS Privacy Office would like to commend USCIS for their availability, responsiveness, and transparency throughout the PCR process, and would like to thank the USCIS Privacy Office in particular for their assistance in conducting this PCR. PRIV looks forward to working with USCIS in the future to provide any and all support needed to assist in implementing these recommendations.

V. Privacy Compliance Review Approval

Responsible Official

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

Approval Signature

[Original signed copy on file with the DHS Privacy Office.]

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security