Privacy Impact Assessment Update
for the

FOIA/PA Information Processing System (FIPS)

DHS/USCIS/PIA-038(b)

May 31, 2018

Contact Point
Donald K. Hawkins
Privacy Officers
U.S. Citizenship and Immigration Services
(202) 272-8030

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

Abstract

U.S. Citizenship and Immigration Services (USCIS), a component of the Department of Homeland Security (DHS), operates the Freedom of Information Act/Privacy Act (FOIA/PA) Information Processing System (FIPS) to process Freedom of Information Act and Privacy Act requests from any person or entity requesting access to USCIS records. FIPS is being decommissioned and a new system is being designed and developed, named the FOIA Immigration Records System (FIRST), which will ultimately replace FIPS. USCIS is releasing a public-facing portal of FIRST for requesters who choose to receive records electronically, enabling the viewing and downloading of responsive FOIA/PA records. USCIS is conducting this Privacy Impact Assessment (PIA) update to analyze the privacy impacts associated with the public-facing portal of FIRST.

Overview

The Freedom of Information Act of 1966, as amended,[1] permits any person to request access to federal agency records. The FOIA establishes a presumption that records in the possession of federal departments and agencies are accessible, except to the extent that the records are protected from disclosure by any of the nine exemptions contained in the law or by one of three special law enforcement record exclusions.[2]

The Privacy Act of 1974, as amended,[3] embodies a code of fair information principles that govern the collection, use, maintenance, and dissemination of personally identifying information (PII) about individuals, defined as U.S. citizens or lawful permanent residents (LPR), which is maintained in a system of records by federal departments. The Privacy Act provides, among other things, U.S. citizens and LPRs with the right to request access to federal department and agency records that are maintained on them. USCIS manages its Freedom of Information Act and Privacy Act (FOIA/PA) program in accordance with the FOIA, the Privacy Act, DHS regulations, and DHS policy. Individuals, as defined under the PA, may request PA-protected records about themselves; however, records may be exempt from access, amendment, or correction depending on the System of Records.[4]

FIPS

USCIS Immigration Records and Identity Services (IRIS) Office of Records Services has historically used FIPS to efficiently and effectively respond to FOIA/PA requests. FIPS uses

[1] 5 U.S.C. § 552.
[2] The nine exemptions and three exclusions are available at www.dhs.gov/foia.
[3] 5 U.S.C. § 552a.
[4] The Privacy Act of 1974 (5 U.S.C. § 552a) exemptions can be found in Section (j) and (k) of the Act at www.uscis.gov.

document imaging, workflow, and web-server technologies to manage the FOIA/PA case life cycle for USCIS. FIPS allows for a flexible workflow, first-in-first-out processing, and accurate audit trails. USCIS personnel and contractors are able to review and process electronically scanned images of documents responsive to FOIA/PA requests to ascertain whether FOIA or Privacy Act exemptions may be applied.

FIPS is also used to generate automated letters and reports. Automated letter types include acknowledgment, blank,[5] expedited processing denial, final action, still interested, payment, redirect, referral, referral memo to a DHS component, remand memo, specialty (lost file and track 3 denial),[6] staffing,[7] status, and supplemental release.[8] The automated reports are categorized according to the type of information they present. The following reports are for internal management use only:

- Annual reports for DHS annual reporting requirements (e.g., FOIA Annual Report);
- Appeals reports to manage and report on appealed cases;
- Balanced Scorecard reports to report balanced scorecard metrics;
- Detailed reports provide case lists of pending, unassigned cases;
- Management reports to help managers monitor workloads, determine resource needs, and recognize problem areas;
- Summary reports to provide management and analysis information; and
- Troubleshooting reports to identify potential problems.

FIPS stores three categories of information: (1) biographical data, such as the requester's name, address, and Alien Number (A-Number); (2) correspondence to and from the requester and with federal offices; and (3) electronic images of USCIS records that are responsive to the FOIA/PA request. FIPS also includes indexing information, such as case and document control numbers (within the system) and classification information, such as the source and type of the request. None of the information is shared with other systems. Only those USCIS employees and contractors assigned to handle FOIA/PA requests and contractors who administer the system's technical functions have access to the system.

[5] Blank letters allow for FOIA/PA staff to customize letters based on specific situations.
[6] Track 3 is for cases with pending immigration court proceedings. Track 3 denial letters are considered specialty letters that inform the requester that his or her request for faster service has been denied.
[7] A staffing letter is an internal letter that USCIS provides to the office that holds the requested file or document.
[8] A supplemental release is when USCIS responds after an initial response was sent out. More documents may have been discovered and processed or documents may have been reprocessed.

FOIA/PA Request Process

Historically, the flow of information through FIPS begins with receiving a written request for access to records, by either completing Form G-639, *Freedom of Information Act/Privacy Act Request*, or sending a written letter by mail, fax, or email.[9] Requests are first scanned or converted into electronic images, then indexed and converted into a case file that is assigned a computer-generated control number that is used for tracking purposes. The control number is generated based on sequential order as the cases are created. FOIA/PA staff then use FIPS to generate an acknowledgment letter that is sent to the requester informing the requester that his or her request has been received and providing the requester with the control number that is used on all further correspondence concerning the request.

For PA requests specifically, when individuals seek records from a USCIS system of records or any other DHS system of records, their request must conform to the Privacy Act regulations set forth in 6 CFR part 5. In order for USCIS to verify the information submitted by the requester against the information contained within USCIS records, individuals must provide their full name, current address, date of birth, and place of birth. Individuals are also required to reasonably describe the information being requested. Individuals must sign their request and their signature must be either notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. Individuals may also submit additional information, such as phone numbers, fax number, certificates (e.g., birth, death, and marriage), email address, or A-Number, to help USCIS facilitate the processing of the FOIA/PA request in the most efficient manner. Any additional information submitted by requesters allows the Office of Records to identify and locate records more expeditiously. USCIS does not request Social Security numbers (SSN) and individuals are not required to submit such information.

The information provided by the requester is entered into FIPS and used to assist in identifying and locating the specifically requested material. This information is also matched to information in the actual file to verify the requester's identity, and this verification is documented in a case note within FIPS.

FOIA/PA staff search for records responsive to the request by using other USCIS systems that house official immigration records. For example, the Office of Records can request a copy of the paper Alien File (A-File)[10] from the office where the paper A-File resides or records can be

[9] The Form G-639 and submission instructions are available at https://www.uscis.gov/g-639.
[10] The A-File is a paper or electronic file that contains official immigration records of aliens or persons who are not citizens or nationals of the United States, as well as U.S. born citizens involved in certain immigration crimes. A-Files contain all records pertaining to naturalized citizens and any active case of an alien not yet naturalized, including records created as he or she passes through the U.S. immigration and inspection process and, when applicable, records related to any law enforcement action against or involving the alien.

retrieved or downloaded through the Enterprise Document Management System (EDMS)[11] or USCIS Electronic Information System (USCIS ELIS).[12]

When the responsive records (e.g., A-File content) are delivered to FOIA/PA staff, they are scanned into electronic images and saved in FIPS. The FOIA/PA staff then process the case by reviewing each of the responsive records and redacting any information that is exempt from disclosure according to provisions of either the FOIA or the Privacy Act.

After the final review of the responsive records is complete, FOIA/PA staff use FIPS to generate a cover letter to send with the responsive, non-exempt records to the requester. FIPS generally saves the records to a compact disk (CD) and provides that CD to the requester, unless the requester requests that the responsive records be returned in paper format.

Reason for the PIA Update

USCIS has historically relied on a paper-based process to receive and respond to FOIA/PA requests. As part of the modernization effort, USCIS is moving to process FOIA/PA records electronically. FIRST is being developed and deployed in several phases as the development of each functionality is completed. USCIS is releasing a public-facing portal of FIRST to enable the viewing and downloading of responsive FOIA/PA records. This portal has an application-programming interface that makes it compatible with FIPS. During the modernization effort, USCIS will continue to use FIPS and FIRST concurrently. Once FIRST is fully operational and reliable, all information from FIPS will be transferred to FIRST, and the FIPS system will then be decommissioned. Once fully operational, USCIS will retire the USCIS FIPS PIA and all associated updates and replace them with a FIRST PIA.

Migration to Cloud-based Platform

USCIS is undergoing a legacy system modernization effort to align with the Office of Management and Budget (OMB) "Cloud First" policy in order to improve business operations.[13] When evaluating options for new IT deployments, OMB requires that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. FIRST operates on the Amazon Web Services (AWS) cloud platform. This migration does not impact the collection and use of PII in FIRST or FIPS. USCIS requires AWS to segregate FIRST data from all other third-party data. All existing records from FIPS will be extracted from the legacy database and transferred to the new cloud environment. This technological advancement does not impact the

[11] *See* DHS/USCIS/PIA-003 Integrated Digitization Document Management Program and subsequent updates, *available at* https://www.dhs.gov/publication/dhsuscispia-003a-integrated-digitization-document-management-program.
[12] *See* DHS/USCIS/PIA-056 USCIS Electronic Immigration System, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-elisappendixaupdate-may2018.pdf.
[13] 25 Point Implementation Plan to Reform Federal Information Technology Management (December 9, 2010), *available at* https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

collection and use of records in FOIA/PA, but rather modifies the way USCIS stores and maintains FOIA/PA records.

FIRST Digital Release Portal

In May 2018, USCIS is implementing a public-facing portal for requesters who choose to receive their responsive records electronically. This portal is hereinafter referred to as the "Digital Release portal." At this time, USCIS will continue processing FOIA/PA requests using the internal FIPS platform; however, USCIS will now give the requester the option of viewing and/or downloading the responsive records via the public-facing Digital Release portal within FIRST, as opposed to receiving them by CD or in paper form. To receive the responsive documents electronically, the requester must opt-in to the process; otherwise the process defaults to receiving responsive documents through the current mail process.

Although the eventual goal is for USCIS to both receive and respond to FOIA/PA requests electronically, this update only introduces the option of electronically delivering responsive documents after a requester chooses the electronic response option. Further updates are planned that will include an electronic method of submitting FOIA/PA requests. As described above, to make a FOIA/PA request, the requester is still required to complete a paper Form G-639, *Freedom of Information Act/Privacy Act Request*, or send a written request by mail, fax, or email.

Once USCIS receives the request, it is converted into a case file in FIPS and FOIA/PA staff generates an acknowledgment letter that is sent to the requester via the United States Postal Service (USPS) to the postal address listed on the request. The acknowledgment letter informs the requester that his or her request has been received and provides the requester with the control number that is used for all further correspondence concerning the request.

As part of this update, the acknowledgment letter now lists multiple options available for the requester to receive responsive records (i.e., through the Digital Release portal or through USPS mail). Should the requester prefer to receive responsive records electronically, the requester must opt-in for an electronic delivery by actively registering his or her FOIA/PA request to his or her USCIS online account. The acknowledgement letter provides instructions for (1) creating a USCIS online account for viewing and retrieving the responsive records, and (2) using the control number and a Personal Identification Number (PIN) to associate the USCIS online account to responsive records within FIRST.[14] If the requester chooses to receive the responsive records online, he or she will then receive an email notification when the responsive records are available in the Digital Release portal.

[14] Currently, the PIN does not expire if the requester does not opt-in to electronic delivery. However, if the requester does not opt-in, the responsive records are sent via mail, and there would be no records in the Digital Release portal for the requester to view if he or she accessed the portal at a later date.

If the requester does not opt-in to receiving responsive records electronically, the records will be mailed to the requester on a CD, as is the current practice.

Account Creation for Digital Release Portal

In addition to the instructions provided on the acknowledgment letter, the USCIS FOIA/PA request web page will also have a link to the FIRST Digital Release portal.[15] If the requester has an existing USCIS online account, he or she will not be required to create a new one to access the Digital Release portal. The requester can use his or her current account login and password information, and keep his or her current account preferences. The FIRST Digital Release portal will leverage the Public USCIS Identity, Credential, and Access Management (ICAM) program. ICAM Public is the enterprise-wide program that manages identity, credential, access and federation for USCIS online accounts, and provides external users access to USCIS systems electronically. FIRST is integrated with ICAM using Security Assertion Markup Language (SAML) protocols. SAML works by transferring the user's identity from one place (the identity provider) to another (the service provider). ICAM is acting as the Identity Provider (IdP) and FIRST as the Service Provider.

If a requester does not have a USCIS online account, the requester will be directed to ICAM Public to create one.[16] To create an account, an individual enters an email address into an online form. USCIS sends a confirmation email to the provided address for accuracy. The email address is then stored as the account holder's username. The account holder is required to create a strong password, and provide "fill-in-the-blank" answers to security questions if he or she needs to reset the account password in the future. USCIS provides the account holder with a dropdown menu of standard questions, and the account holder chooses which ones to answer as security questions. USCIS does not use the answers to these questions for purposes other than assisting with password resets.

USCIS online account passwords and answers to the security questions are centrally stored within ICAM Public. Passwords are not visible to USCIS. The answers to the security questions are only visible to USCIS customer helpdesk personnel who assist account holders in resetting their passwords.

USCIS has established secured gateways to ensure that the individual's USCIS online account only has access to his or her responsive FOIA/PA records contained in the Digital Release portal within FIRST.

[15] https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia/uscis-freedom-information-act-and-privacy-act.
[16] https://myaccount.uscis.dhs.gov/.

Multi-Factor Authentication and Identity Verification

The USCIS online account is created through ICAM Public and only connects to FIRST without sharing any account information. To complete account creation and ongoing access to FIRST via ICAM Public, USCIS sets a two-factor authentication code preference for integrity and authenticity assurance purposes. FIRST is integrated with ICAM account and role management and security services. The Digital Release portal will leverage ICAM Public's authentication services at a National Institute of Standards and Technology (NIST) authentication assurance level 2 (AAL2). AAL2 provides high confidence that the account holder controls the authenticator(s) bound to account, such as mobile phone number, authenticator application, or email address. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols.

Each time the requester logs in, FIRST forwards an authentication code through an email, text message, or through the use of a third-party authenticator application as part of account holder's credentials. The user credentials are sent to the ICAM Public system for verification and authentication.

Since the implementation of the Digital Release portal does not include online submission of FOIA/PA requests, USCIS is not changing its current process for identity verification of the requester in regards to verifying the information submitted by the requester against the information contained within USCIS records. This verification process is completed outside of FIRST. The remote identity verification of the requester will be a capability developed in a future release and as functionalities are added to FIRST. USCIS will assess the use of technologies, risks, and adherence to DHS policies and NIST guidance during the development process and in the FIRST PIA.

Registering FOIA/PA Request within FIRST

After the account is established in ICAM Public, the account holder will be able to associate the responsive records to his or her USCIS online account using the control number and PIN as provided in the acknowledgment letter. The control number and PIN are only needed one time in order to associate the responsive records to the USCIS online account. Information within the requester's Digital Release portal can only be accessed by the requester as the Digital Release portal does not allow the requester to transfer responsive records to another account. However, should the requester wish to share his or her responsive records, then the requester has the option of printing the documents or saving the documents to his or her personal device. Responsive records are "pushed" through a one-way encrypted secured socket layer to the Digital Release portal in FIRST from FIPS, where the records reside.

Privacy Impact Analysis

Authorities and Other Requirements

The legal authority to administer USCIS' FOIA/PA program does not change with this update. USCIS is authorized to collect this information per the Freedom of Information Act of 1966, as amended (5 U.S.C. § 552), the Privacy Act of 1974, as amended (5 U.S.C. § 552a), Departmental Regulation (5 U.S.C. § 301), 6 CFR Part 5, and Records Management by Federal Agency Heads (44 U.S.C. § 3101).

The DHS FOIA and Privacy Act Record System SORN[17] continues to cover the collection, maintenance, and use of the information to support the processing of record access requests and administrative appeals under the FOIA, as well as access, notification, and amendment requests and administrative appeals under the Privacy Act. The collection of information associated with FIRST is still compatible with the purpose of the DHS FOIA and Privacy Act Record System SORN because the collection and use of information permits USCIS to administer its FOIA/PA program and carry out its responsibilities under the FOIA/PA.

FIRST is also covered by the DHS E-Authentication Records System of Records,[18] which covers information collected to create and authenticate an individual's identity for the purpose of obtaining a credential to electronically access a DHS program or application.

This PIA update does not change the Authority to Operate (ATO) for FIPS or FIRST. FIPS–now FIRST–was granted an authority to operate (ATO) on October 29, 2015, and is part of the Ongoing Authorization (OA) program. FIRST is a modernization of FIPS and because the system is a part of the OA program that has a continuous ATO, a new ATO is not needed for the implementation of the Digital Release portal. However, with each phase of modernization this application must be fully documented and assessed to ensure the security posture of the system. Ongoing Authorization requires FIPS and FIRST to be reviewed on a monthly basis to ensure compliance with security and privacy requirements in order to maintain its ATO.

The records schedule does not change with this update. FOIA/PA correspondence and supporting documentation will be retained in accordance with the National Archive and Records Administration's (NARA) General Record Schedule 4.2. FOIA/PA request records are maintained for a period of 6 years plus one day from the final agency action or 3 years and one day after final adjudication by the courts, whichever is later. Once released to the requester, the responsive records are not governed by a NARA-approved schedule or required to adhere to the Federal Records Act.

[17] *See* DHS/USCIS-001 DHS FOIA and Privacy Act Record System, 79 FR 6609 (February 4, 2014).
[18] *See* DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

After 90 days, the responsive records will no longer be readily available in the Digital Release portal and will be automatically archived and stored in FIPS.[19] Requesters also have the ability to self-archive responsive records, which removes the records from the requester's active list. Responsive records may be restored to the active list by the requester. For responsive records that have been available for viewing in the Digital Release portal for more than six months beyond the original availability date, FIRST automatically notifies the requester that the responsive records they are about to view are only current as of the date the request was made. The requester is then asked, given the age of the records, if they want to proceed with reviewing the records.

This PIA update does not impact the Paperwork Reduction Act (PRA) requirements for the FOIA/PA Program. Collection of information for the FOIA/PA Program is covered by the Paperwork Reduction Act, specifically, by OMB Control number 1615-0102 (Form G-639, *Freedom of Information/Privacy Act Request*).

Characterization of the Information

In addition to the information described in DHS/USCIS/PIA-038 and subsequent updates, the public can create a USCIS online account to retrieve responsive records. During the account creation process, USCIS collects information related to the account, such as user name that is an email address (used to contact the individual), password, and challenge questions.

For authentication purposes, USCIS requires individuals to provide an email address and short message service (SMS) number, for sending one-time PIN to be used as a second factor in authenticating. ICAM Public will allow individuals to use a third-party authenticator application (e.g., Google Authenticator, Authy, Microsoft Authenticator) to provide two-factor authentication into their USCIS online account. The types of responsive records obtained from USCIS systems have not changed with this update. With this enhancement, USCIS may continue to release records that may include the following personally identifiable information:

- Name;
- Date of Birth;
- SSN (or other number originated by a government that specifically identifies an individual);
- Photographic Identifiers (e.g., photograph image, x-rays, and video tapes);
- Driver's License;
- Biometric Identifiers (e.g., fingerprint and voiceprint);
- Mother's Maiden Name;

[19] Public Law 113-187, The Presidential and Federal Records Act Amendments of 2014.

- Vehicle Identifiers (e.g., license plates);
- Mailing Address;
- Phone Numbers (e.g., phone, fax, and cell);
- Certificates (e.g., birth, death, and marriage);
- Legal Documents or Notes (e.g., divorce decree, criminal records, or other);
- Email Address;
- Education Records;
- A-Number; and
- Financial Records.

This PIA update does not impact the sources of information, how the information is collected, or how the accuracy of data is ensured as outlined in DHS/USCIS/PIA-038 FIPS, published on June 14, 2011. FIRST does not use information from commercial sources or publicly available data.

Privacy Risk: There is a risk that FIPS, FIRST, or ICAM collects more information than necessary in order to release FOIA/PA responsive documents through the Digital Release portal.

Mitigation: This risk is fully mitigated. As part of the implementation of the Digital Release portal, FIRST is not collecting any new PII. The identity verification process completed by USCIS as part of the FOIA/PA request process occurs outside of FIRST, as described above and originally outlined in DHS/USCIS/PIA-038 and subsequent updates. USCIS will continue to only collect the minimum amount of information necessary for the purpose of responding to a FOIA/PA request (as consistent with 6 CFR part 5). USCIS uses this information to verify the information submitted by the requester against the information contained within USCIS records.

Regarding the collection of authentication-related information, an individual's account is created through ICAM Public and only connects to FIRST without sharing any account information. FIRST will display the responsive documents that may contain sensitive PII, but only after the requester's identity has been verified and presented a valid credential to access the information.

Privacy Risk: There is a risk that information collected from the requester or information contained within the responsive records may be inaccurate.

Mitigation: This risk is partially mitigated. The risk of inaccurate information is reduced by collecting contact information directly from the requester. Information entered into FIPS undergoes three levels of review to ensure the accuracy of information. Once FIRST is fully deployed, it will undergo the same review process.

FOIA and PA requests depend on the originating office for the accuracies of the responsive record. However, if information is discovered to be inaccurate, requesters can amend their record accordingly.

Uses of the Information

With this update, USCIS continues to use information to administer USCIS' FOIA/PA program. With the Digital Release portal USCIS will:

(1) Verify the identity of the requester

As a result of this PIA update, USCIS is not changing its current process for identity verification of the requester in regards to verifying the information submitted by the requester against the information contained within USCIS records. Individuals submitting FOIA or PA requests may submit all or some of the following information:

- Name;
- Date of Birth;
- Mailing Address;
- Phone Numbers (e.g., phone, fax, and cell);
- Certificates (e.g., birth, death, and marriage);
- Email Address;
- A-Number; and
- Country or Place of Birth.

This information, which is provided directly by the individual, is entered into FIPS and manually verified. The only mandatory information for identity verification purposes is the requester's name, mailing address, date of birth, and place of birth. Any additional information provided is used to help USCIS facilitate the processing of the FOIA/PA request in the most efficient manner. Any additional information submitted by requesters allows the Office of Records to identify and locate records more expeditiously.

(2) Establish a secure online account in order to receive responsive FOIA/PA documents through the Digital Release Portal

If records responsive to the request exist, they are analyzed for releasability, i.e., a determination as to whether any mandatory or discretionary prohibitions or exemptions exist. Releasable documents are ultimately enclosed with a letter to the requester itemizing the records and identifying what, if any, exemptions are claimed to withhold portions of the records either from the FOIA or PA. In order to establish an online account to receive responsive records, USCIS

collects information related to the account, such as user name that is an email address (used to contact the individual), password, and challenge questions.

For authentication purposes, USCIS requires individuals to provide an email address and SMS number for sending one-time PIN to be used as a second factor in authenticating. ICAM Public will allow individuals to use a third-party authenticator application (e.g., Google Authenticator, Authy, Microsoft Authenticator) to provide two-factor authentication into their USCIS online account.

Privacy Risk: There is a risk that FIRST will inadvertently disclose information about a different individual by uploading the incorrect FOIA/PA responsive documents to the Digital Release portal.

Mitigation: This risk is fully mitigated. The control number and PIN (as provided in the acknowledgment letter) used to link the responsive records to the requester are directly associated with the control number of the FOIA/PA request. Responsive records cannot be transferred to any other requester within the Digital Release portal.

Privacy Risk: There is a risk that an individual will gain unauthorized access to the requester's responsive records in the Digital Release portal.

Mitigation: This risk is partially mitigated. There is a chance that an individual could intercept the acknowledgment letter that contains the control number and PIN. If the requester already has a USCIS online account, then the unauthorized individual would also have to know the requester's user name and password to gain access to the Digital Release portal in FIRST. If the requester does not have a USCIS online account, then that unauthorized individual could set up an account to gain access to the requester's responsive records through the Digital Release portal. To mitigate this risk, USCIS uses multi-factor authentication. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols.

Notice

This PIA update provides general notice to the public that FIRST is modernizing FIPS to serve as the primary case management system for the administration of USCIS' FOIA/PA program. This PIA update also provides notice describing the changes to information storage and maintenance practices by USCIS as data is migrated to the AWS public cloud platform. USCIS continues to provide notice to individuals through the associated Privacy Notices[20] and the associated SORNs. Additionally, USCIS is providing notice through the acknowledgment letter sent to requesters and on USCIS' FOIA website.[21] Lastly, USCIS is developing a public marketing

[20] A Privacy Notice is included on Form G-639, *Freedom of Information Act/Privacy Act Request*, and on the ICAM Public Account Creation page (https://myaccount.uscis.dhs.gov/).
[21] https://www.uscis.gov/about-us/freedom-information-and-privacy-act-foia/uscis-freedom-information-act-and-privacy-act.

strategy, which may include press releases, social media outreach, and mailing out informational brochures.

Privacy Risk: There is a privacy risk that individuals providing information to USCIS do not receive sufficient notice that explains their information is being stored on a server not owned or controlled by USCIS.

Mitigation: This risk is partially mitigated. USCIS is providing notice through the publication of this PIA update. USCIS also provides notice to individuals about the collection and use of their information. USCIS, however, does not provide explicit notice that the information may be stored in a cloud-based system at the time of collection. Regardless of storage location of records, FIRST records are governed by USCIS policies concerning the collection, use, and dissemination of personally identifiable information. USCIS remains accountable for the records it collects.

Data Retention by the project

This PIA update does not affect the data retention for responsive FOIA/PA records. Responsive records will reside in FIPS and are maintained by USCIS in accordance with the NARA General Record Schedule 4.2. Records are maintained for a period of 6 years plus one day from the final agency action.

Responsive records available on the Digital Release portal will be automatically archived in FIPS after 90 days. Requesters also have the ability to self-archive responsive records, which removes the records from the requester's active list. Responsive records may be restored to the active list by the requester. For responsive records that have been available for viewing in the Digital Release portal for more than six months beyond the original availability date, the requester is provided a message, prior to viewing the responsive records, that highlights the fact that the responsive records he or she is are about to view are only current as of the date the request was made. The requester is then asked, given the age of the records, if he or she wants to proceed.

If the requester's USCIS online account becomes inactive, then the requester would be required to reactivate his or her USCIS online account to gain access to the Digital Release portal.

Privacy Risk: There is a risk that the responsive records may be retained in FIRST longer than necessary.

Mitigation: This risk is mitigated. Responsive records will be automatically archived in FIPS after 90 days. Once the retention period is met (6 years plus the current year from when the user logs into the account), the records are deleted. This retention schedule is brief enough to ensure privacy protection, but long enough to ensure the operational integrity of the FOIA and PA program.

Information Sharing

This PIA update for the Digital Release portal functionality does not impact the internal and external sharing in FIRST. USCIS continues share information as described in Sections 4.0 and 5.0 of the DHS/USCIS/PIA-038 FOIA/PA Information Processing System (FIPS), published on June 14, 2011.

Redress

This PIA update does not impact how access, redress, and correction may be sought through USCIS, but does change how an individual receives records responsive to his or her request. With this update, USCIS continues to provide individuals with access to their information through a FOIA/PA request, and individuals may now receive responsive records electronically through the Digital Release portal.

Auditing and Accountability

USCIS ensures that practices stated in this PIA update comply with federal, DHS, and USCIS policies and procedures, including standard operating procedures, orientation, and training, rules of behavior, and auditing and accountability procedures. FIRST is maintained in the Amazon Web Service (AWS), which is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines.[22] AWS is FedRAMP-approved and authorized to host PII.[23] FedRAMP is a U.S. Government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

USCIS employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process. These technical and security controls limit access to USCIS users and mitigate privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further, DHS security specifications also require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

Privacy Risk: There is a potential security risk because data is stored on third-party servers, which may not have been assessed by USCIS security compliance personnel to ensure compliance with federal IT security requirements.

[22] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[23] https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.

Mitigation: USCIS cloud service providers must be FedRAMP certified. By using FedRAMP-certified providers, USCIS leverages cloud services assessed and granted provisional security authorization through the FedRAMP process to increase efficiency while ensuring security compliance. Additionally, before using AWS, USCIS verified through a risk assessment that AWS met all DHS privacy and security policy requirements. Further, all cloud-based systems and service providers are added to the USCIS Federal Information Security Modernization Act (FISMA) inventory and are required to undergo a complete security authorization review to ensure security and privacy compliance. As part of this process, the DHS Senior Agency Official for Privacy reviews all FedRAMP cloud service providers for privacy compliance and privacy controls assessments as part of the privacy compliance review process.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

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

_____

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