1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) **Date PIA was completed:** December 1, 2011

(b) **Name of system:** Visa Opinion Information Service

(c) **System acronym:** VOIS

(d) **IT Asset Baseline (ITAB) number:** 875

(e) **System description (Briefly describe scope, purpose, and major functions):**

The Visa Opinion Information Service (VOIS) provides a graphical user interface (GUI) to the Consular Consolidated Database (CCD). It acts as a toolkit (or "service") to simplify the access, the management, and the analysis of the visa data available in CCD. It supports the Visa Office (VO) business process of rendering security advisory opinions (SAOs) and advisory opinions (AOs). VOIS is a WebForms/ASP.NET implementation that allows for convenient, extensive integration with the data and hypertext markup language (HTML) reports available within CCD. While VOIS mainly functions as an interface to CCD data, it also permits VOIS users to update, modify, add and delete information obtained from CCD within the VOIS database tables. VOIS also allows users to submit name check requests to the CLASS system and requests for clearances from outside information agencies.

VOIS permits Visa Office Coordination Division (L/C) officers, Advisory Opinions Division (L/A) officers, Public Inquiry (P/I) officers, and the Bureau for Population, Refugees, and Migration (PRM) to access CCD and consult with numerous other government agencies that often have relevant information pertaining to visa applicants. Through VOIS, L/C users can quickly and accurately complete their mission-critical task of compiling the information necessary to form an accurate security advisory opinion (SAO) on visa applicants. Similarly, VOIS provides L/A users the ability to quickly and efficiently respond to requests for legal advisory opinions (AO) from posts throughout the world and permits P/I users to access inquiries from the public and to access real-time case data and document control features. Office of Information Management and Liaison (VO/I) users can also use VOIS to receive, review, and respond to requests to delete hits from the CLASS system (via CLOK SAOs).

The service tracks all actions surrounding an SAO/AO from the point the record is received in VOIS to the point when it is completed and archived. All user actions on the SAO/AO are audited at the database level. All system actions on an SAO/AO, such as updates from CCD, are captured and tracked. When a user sends a response to an SAO/AO request, the text of the response will be stored in CCD and will be available for viewing. Multiple VOIS users can view the same VOIS document simultaneously, but only one user can edit an SAO/AO at a time.

Users can use the available scanning workstations located in the Visa Office (VO) and the Visa File Room (VFR) to scan documents into CCD for access by VOIS. A scanner is used to take a picture of a paper document and convert that picture into data, which is stored electronically. VOIS allows for these scanned documents to be associated with an SAO/AO or applicant record. As part of CCD, VOIS is a Sensitive But Unclassified (SBU) service, and therefore, classified material is restricted from being scanned into or stored in CCD via VOIS. A standard warning message regarding the SBU guideline is displayed when users authenticate to CCD. VOIS provides the capability for users to note that additional classified information outside the automated service is available on an applicant/SAO/AO, without divulging any classified data. This capability can be used to indicate an external source of information that may be classified. All classified information is manually managed and filed in the VFR.

Because VOIS is a front-end application to CCD, VOIS users must first authenticate using the CCD Portal application before accessing VOIS.. Consequently, CCD handles the primary logon and assignment of VOIS user roles.

(f) **Reason for performing PIA:**

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(g) **Explanation of modification (if applicable):** N/A

(h) **Date of previous PIA (if applicable):** September 2009

3. Characterization of the Information

The system: ***VOIS collects PII that falls under the provisions of the E-Government Act and Privacy Act.***

☐ Does NOT contain PII. If this is the case, you must only complete Section 13.

☒ Does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The vast majority of information stored in VOIS is data on foreign nationals collected as part of the U.S. visa application process. As such, the information stored in VOIS is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

The data on foreign nationals includes name, address and telephone number, nationality, birth date, gender, birth country, passport number, passport issuance, expiration information, and biometric data to include fingerprints and photographs.

Because visa applicants themselves are not U.S. persons (that is, U.S. citizens or an alien lawfully admitted for permanent residence), they are not covered by the provisions of the E-Government Act of 2002 or the Privacy Act of 1974, as amended.

Once an individual has received a diversity visa, he or she may apply for citizenship through the Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS) to become a citizen. Applicants and their family members may apply before entering the United States; the Department of State applies the full coverage of the Privacy Act of 1974, as amended, and any other laws or memoranda that may cover a United States citizen's right to privacy. However, a visa record may include personally identifiable information (PII) about persons associated with the foreign national visa applicant who are U.S. citizens or aliens lawfully admitted for permanent residence.

This PII on U.S. citizens may include the following: U.S. sponsor's name, address and phone number; U.S. contact name, address and phone numbers; and employer name, address and phone numbers. The source of information is the visa applicant, petitions, and visa applications.

b. How is the information collected?

VOIS receives data from Consular systems domestically, at posts, and from external government agencies such as the Social Security Administration. It collects visa data via the DS-160 and DS-260 (online forms.)

c. Why is the information collected and maintained?

The information is collected to determine the eligibility of foreign nationals who have applied or are applying for U.S. visas to travel to the United States and to provide a means to contact the applicant.

d. How will the information be checked for accuracy?

Accuracy is the responsibility of the government agency that collected the data originally and the applicant supplying the information. Any errors detected by CCD are called to the attention of the collecting agency.

A Data Engineering team monitors the databases to insure exact duplicate replications and consistent accuracy. Identical software is installed, and configuration management controls are in place for all databases. To verify accuracy, all data updates are compared against existing data prior to being applied, and any discrepancies are reported and investigated.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- Immigration and Nationality Act (INA) 1952, 8 U.S.C. 1101, as amended
- INA, 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- INA, 8 U.S.C. 1202(f) (Confidential Nature of Visa Records)
- 22 U.S.C 2651(a) (Organization of Department of State)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996
- (IIRIRA96)
- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705

- Executive Order 11295 (August 5, 1966)
- Sec. 599C of Public Law 101–513, 104 Stat. 1979, as amended (Claims to benefits by virtue of hostage status);
- 22 U.S.C. 5501–5513 (Aviation disaster and security assistance abroad; mandatory availability of airline passengers manifest);
- 22 U.S.C. 4215, 4221 (Administration of oaths, affidavits, and other notarial acts);
- 28 U.S.C. 1740, 1741 (Authentication of documents);
- 28 U.S.C. 1781–1783 (Judicial Assistance to U.S. and foreign courts and litigants);
- 42 U.S.C. 14901–14954; Intercountry Adoption Act of 2000, (Assistance with intercountry adoptions under the Hague Intercountry Adoption Convention, maintenance of related records);
- 42 U.S.C. 11601–11610, International Child Abduction Remedies Act (Assistance to applicants in the location and return of children wrongfully removed or retained or for securing effective exercise of rights of access);
- 22 U.S.C. 4802 (overseas evacuations).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The personal data collected by VOIS is the minimum necessary to carry out the function of VOIS as identified in Section 3(c) above.

Due to the strict security controls required by all Department of State systems before system operation commences, privacy risks are generally limited to three categories. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft:

- **Device theft or loss** Lost or stolen laptops and other devices such as removable drives may contain PII.

- **Portable Devices** PII is at the fingertips of every staff member who has email, database and Web access at work. The growing use of removable media such as USB drives, CDs/DVDs and portable Mp3 players creates risk by making PII easily transportable on devices that aren't always properly secured.

- **Insider threat** Disgruntled employees seeking revenge or inadvertent human error to send PII over the internet.

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act of 2002 and information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (eg, firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

VOIS aids the Department in processing visa applications and determining whether visa issuance is appropriate. The service tracks all actions surrounding an SAO/AO from the point the record is received in VOIS to the point when it is completed and archived. All user actions on the SAO/AO are audited at the database level. All system actions on an SAO/AO, such as updates from CCD, are captured and tracked. When a user sends a response to an SAO/AO request, the text of the response will be stored in CCD and will be available for viewing. Multiple VOIS users can view the same VOIS document simultaneously, but only one user can edit an SAO/AO at a time.

b. What types of methods are used to analyze the data? What new information may be produced?

Through VOIS, L/C users can quickly and accurately complete their mission-critical task of compiling the information necessary to form an accurate security advisory opinion (SAO) on visa applicants. Similarly, VOIS provides L/A users the ability to quickly and efficiently respond to requests for legal advisory opinions (AO) from posts throughout the world and permits P/I users to access inquiries from the public and to access real-time case data and document control features. Office of Information Management and Liaison (VO/I) users can also use VOIS to receive, review, and respond to requests to delete hits from the CLASS system (via CLOK SAOs).

The service tracks and records all actions surrounding an SAO/AO from the point the record is received in VOIS to the point when it is completed and archived. All user actions on the SAO/AO are audited at the database level. All system actions on an SAO/AO, such as updates from CCD, are captured and tracked. When a user sends a response to an SAO/AO request, the text of the response will be stored in CCD and will be available for viewing. Multiple VOIS users can view the same VOIS document simultaneously, but only one user can edit an SAO/AO at a time.

In addition, no data mining is used to analyze the data stored in VOIS.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Some U.S. citizen information stored by CCD is obtained through commercial databases and public records such as names, addresses, birth dates, race, identification numbers (e.g. social security numbers) and country of origin. This data is used to support national security, U.S. border security, official government business or federal law enforcement.

The information obtained through CCD is verified and checked for accuracy by CCD. For more information, please see the CCD PIA.

d. Are contractors involved in the uses of the PII?

All VOIS data is stored in database tables within the CCD environment. CCD is a government-owned system. However, development and support to CCD is provided by contract employees of the Department of State.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

All VOIS data is stored in database tables within the CCD environment. CCD is a government owned system. It is supported by contract employees, who support Department of State employees in the maintenance of the system.

All users, including external Agency users, are screened prior to their employment with the Department or their respective Agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before being given access to the OpenNet and any CA/CST system, including VOIS, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements

Contractors who support CCD are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors involved in the development and/or maintenance of CCD hardware and software must have a level “secret” security clearance. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation

5. Retention

a. How long is information retained?

Record retention depends upon the type of record involved. Files of closed cases are retired or destroyed in accordance with published record schedules of Department of State and as approved by the National Archives and Records Administration.
Paper records produced by this application are shredded or burned, per internal Department of State requirements for handling visas and Department of State records disposition schedules. The schedules range from 6 months for Visa Case files to permanent for Historical files.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging.
When records have reached their retention end-date, they are immediately handled in accordance with appropriate National Archive and Records Administration (NARA) rules.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The only system that VOIS shares an internal connection with is CCD. Via this interface with CCD, VOIS shares information with the following systems for the purpose of rendering Security Advisory Opinions (SAOs) and Advisory Opinions (AOs).

Name of System	Type of Data	Data Flow
ABIS (FR)	Fraud Watchlist data / Photo Identification data	Bi-directional
ACRS	Consular Fee Transaction data	Bi-directional
ACS+	American Citizen data / Personal Identity data	Bi-directional
CST	Shared Database Tables	Bi-directional
CLASS	Consular Lookout and Support System	Bi-directional
DataShare	Visa and Passport data	Bi-directional
DVIS	Diversity Visa data	Bi-directional
IVIS	Immigrant Visa Information data	Bi-directional
IVO	Immigrant Visa data, Petition data, Visa Allocation data	Bi-directional
NIV	Non-Immigrant Visa data, Visa refusal data	Bi-directional
VOIS	Visa Opinion Information Service	Bi-directional
WRS	Waiver Request System	Bi-directional

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

There is an electronic connection or interface between VOIS and CCD. In general, information is shared by secure transmission methods permitted under internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Interface Control Document (ICD) and

Memorandums of Understanding (MOUs) are used to define and disclose transmission format via OpenNet. Access to electronic files is protected by passwords and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. VOIS mitigates these vulnerabilities by working closely with the sharing organizations to develop secure standard operating procedures for using this data. These procedures are documented in sharing agreements.

Vulnerabilities and risks are mitigated through the system's certification process. NIST recommendations are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

Access to information is controlled by application access controls. User training at the application level is delivered annually in accordance with internal Department of State regulations.

VOIS has formal, documented procedures to facilitate the implementation of its audit and accountability processes. The application produces audit records that contain sufficient information to establish what events occurred and the sources of the events identified by type, location, or subject. System administrators regularly review and analyze the application audit records for indications of suspicious activity or suspected violations of security protocols.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The Visa Opinion Information Service (VOIS) provides a graphical user interface (GUI) to the Consular Consolidated Database (CCD). It acts as a toolkit (or "service") to simplify the access, the management, and the analysis of the data available in CCD to support Advisory Opinion and Security Advisory Opinion processing. Other agencies do not use VOIS, so the information gathered is not shared externally.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Other agencies do not use VOIS.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

As data is not shared externally, no privacy risk arises from external sharing.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems)

- Visa Records. STATE-39

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Information is not collected directly from individuals for specific use in VOIS. However, VOIS accesses information contained in the CCD which includes PII from visa applications.

In addition, the following forms explain the reason for collecting PII, how it will be used, and the effect of not providing the PII. Refer to the Travel.state.gov website, http://travel.state.gov/visa/forms/forms_1342.html, for more details on these forms:

- DS-160
- DS-260

Notice of the purpose, use and authority for collection of visa information submitted is described in the System of Records Notices titled STATE-39, Visa Records.

b. Do individuals have the opportunity and/or right to decline to provide information?

Personal information regarding individuals is not collected directly by VOIS; it is received from external agencies and Department of State overseas and domestic posts. Regarding information collected from forms filed by visa applicants, the applicants have the right to decline to provide PII for use in processing their immigration visa application. Failure to provide the information necessary to process the application may result in the application being rejected.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Information is not collected directly from individuals for specific use in VOIS. However, VOIS accesses information contained in the CCD which includes PII from visa applications. Visa applicants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's disclosed purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

The Visa Opinion Information Service (VOIS) provides a graphical user interface (GUI) to the Consular Consolidated Database (CCD). It acts as a toolkit (or "service") to simplify the access, the management, and the analysis of the data available in the CCD. Information is not collected directly from individuals for specific use in VOIS. However, VOIS accesses information contained in the CCD which includes PII from visa applications.

The information in VOIS is considered a visa record subject to confidentiality requirements under INA 222(f).

Visa applicants may change their information at any time prior to submission of the application to the Consulate or Embassy. Once that is done, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request and this guidance is available to the public in 9 FAM 40.4:

(1) Correspondence previously sent to or given to the applicant by the post;
(2) Civil documents presented by the applicant
(3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

VOIS information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.36.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

To the extent information in VOIS may be Privacy Act-covered, the notification mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements.

Therefore this category of privacy risk is appropriately mitigated in VOIS.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Because VOIS is a front-end application to CCD, VOIS can only be accessed by way of CCD. Consequently, CCD handles the primary logon. The user must log on to CCD first and then access VOIS. From the CCD personal "welcome" page, VOIS users must click on the Security Advisory Opinion item on the left (blue) panel and several sub-menus will be available. To access VOIS, user can select 'Visa Opinion Information Service' from the sub-menu, and VOIS will launch. CCD will transfer the user's assigned roles and privileges to VOIS. VOIS maximizes the use of the available computational resources by partitioning resource use between CCD, web servers, and client workstations.

Internal access to VOIS is limited to authorized Department of State users, including contractors, that have a justified need for the information in order to perform official duties. To access the system, authorized users must be an authorized user of the State unclassified network. Each domestic organization appoints a certifying authority who is responsible for reviewing each user account request and creating the user account. The certifying authority is also responsible for periodically reviewing the user access list and disabling any user account that no longer requires access.

CCD access for post users is controlled by CST roles granted and managed by CST administrators. Each post has a CST administrator responsible for accepting, reviewing, and creating the individual user accounts.

Once users are properly identified and authenticated by the system, they are authorized to perform all functions commensurate with their official assigned role. CCD employs logical access controls in accordance with the principle of least privilege and the concept of separation of duties.

The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to pass annual computer security and privacy awareness training prior to accessing the system and must complete refresher training in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Therefore, this level of privacy risk is negligible.

Additionally, system audit trails are automatically generated that regularly analyze and review usage in order to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.) As a result of these actions, the residual risk is low.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation

11. Technologies

a. What technologies are used in the system that involves privacy risk?

VOIS is a Government off-the-shelf (GOTS) product and has met required security capabilities, design and development processes, required testing and rigorous internal evaluation procedures and documentation.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No technologies that are known to elevate privacy risk are employed in VOIS. Since VOIS does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum satisfactory in this application.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates VOIS in accordance with information security requirements and procedures required by federal law and internal policy to ensure that information is appropriately safeguarded and protected. The Department of State has conducted a risk assessment of the system, identified appropriate security

controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, its most recent date of authorization to operate was in May 2008 and expires on May 31, 2011 (or upon significant change to the system). We are currently going through the re-authorization process and expect to be certified and accredited through 2014.