1. Contact Information

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: June 4, 2009

(b) Name of system: Visitor Access Control System (Domestic)

(c) System acronym: VACS (D)

(d) IT Asset Baseline (ITAB) number: 876

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

VACS(D) utilizes PassagePoint, a Commercial-Off-The-Shelf (COTS) product developed by Stopware, Inc., which has been used for nearly two years by the information desk staff at Main State entrances to register visitors. A Web Pre-Registration module allows all Department of State (DOS) staff to pre-register single visitors or groups and verify the requestor has escort authority. This module is accessible via the Department's Intranet, OpenNet Plus. The PassagePoint application is currently installed on two DS servers and several client workstations.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): Certification & Accreditation

(h) Date of previous PIA (if applicable):

3. Characterization of the Information

The system:

☐ 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?

VACS(D) allows all DoS staff to pre-register visitors to the Harry S Truman (HST or "Main State") Building. DoS employees may pre-register any non-DoS employees (which may include members of the public and non U.S. persons) for entrance to HST. VACS(D) captures the following data items:

- Name;

- Date of birth;
- Citizenship;
- ID Type (Military ID, Drivers License, Passport Number, Other (could include SSN)); and
- Phone Number.

The information collected by VACS(D) is supplied by the individuals requesting visitor passes and/or law enforcement agencies.

Additionally, VACS(D) collects information on Department of State employees who are hosting the visitors to verify that the requestor has escort authority. VACS(D) collects the following employee information:

- First name;
- Last name;
- Phone number;
- Room number;
- DS Badge number; and
- Bureau.

b. How is the information collected?

Individuals requesting visitor passes for guests fill out a web form online. All information is collected from this online form. This online form is accessible only through the Department of State intranet, OpenNet.

The level of sensitivity of the unclassified information accessed, processed, stored and transmitted on VACS(D) is sensitive but unclassified (SBU). VACS(D) processes privacy data as defined by the Privacy Act of 1974.

c. Why is the information collected and maintained?

The information collected and maintained by VACS(D) is for the purpose of processing visitor requests and managing visitor logs to maintain the safety and security of Department of State facilities.

d. How will the information be checked for accuracy?

The information is verified by receptionists at the Main State Building (HST) upon arrival of each visitor. The receptionist validates that the information entered in the VACS(D) system correctly corresponds with the type and form of identification provided by both the visitor and the escort authority.

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

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to VACS(D), are as follows:

- Pub.L. 99-399(Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended;

- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

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

VACS(D) collects the minimum amount of personally identifiable information necessary to complete its statutorily mandated functions and ensure the ability to identify visitors to the Main State Building (HST) which ultimately supports the safety and security of the facility.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). 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 (e.g., firewalls, intrusion detection systems, antivirus software); and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The information collected and maintained by VACS(D) is used to validate the identity of visitors who desire entry into the Main State Building.

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

Analysis of the information is limited to non-subject-based statistical information, such as the number visitors received by the HST building. Furthermore, no new information is derived.

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

The system does not use any commercial information, publicly available information, or information from other Federal agency databases. All of the information in the system is derived from visitors seeking entry into the HST building.

d. Is the system a contractor used and owned system?

VACS(D) is a U.S. Government-owned system which was primarily designed and developed by contractors. Users of VACS-D are made up of FTE and contracting staff. All personnel are required to abide with regulatory guidelines and have signed and agreed to follow DS's Rules of Behavior.

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.

VACS(D) performs basic internal analytical functions on the PII but does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," where, with the passage of time, PII would be used for purposes for which the public was not given notice. Based on these very specific uses, there is no additional information created about the record subject; therefore, there is minimal privacy risk.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11.

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

The utility of the information in the database about a particular threat will not extend over the allotted time defined in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

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 information collected and maintained by VACS(D) is not shared with any internal organizations.

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

The information collected and maintained by VACS(D) is not shared with any internal or external organizations.

Moreover, numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.

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

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.

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 information collected and maintained by VACS(D) is not shared with any external organizations.

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

The information collected and maintained by VACS(D) is not shared outside the Department of State.

Safeguards in place: VACS(D) is monitored and guided by the inherited security controls of the OpenNet. Controls built into the OpenNet General Support System (GSS), including routers and Network Intrusion Detection System (NIDS), provide network level controls that limit the risk of unauthorized access from all IP segments, to include patch management, configuration management, and segregation of duties.

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

The information that VACS(D) collects is not shared with any external organizations.

Unauthorized and/or unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text) and over an un-trusted communications link can also pose a significant risk. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associated with unauthorized external sharing and unintentional disclosure including, but not limited to formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements (SLA) annual security training, separation of duties, least privilege and personnel screening.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

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

STATE-36

☐ Does NOT contain information covered by the Privacy Act.

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

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-36. Additionally, a Privacy Act Statement is provided at the logon point of the VACS-D web form.

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

Before divulging information via the VACS(D) web form the individual is informed of the Privacy Act statement; the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the System of Records Notice titled STATE-36.

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?

No. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's Disposition Schedule, as defined in Diplomatic Security Records, Chapter 11. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

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 VACS(D)'s purpose and use.

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?

VACS(D) contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual how to inquire about the existence of their records, how to request access to their records, and how to request amendment of their records. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport 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 171.32.

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

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?

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls. The Bureau of Diplomatic Security (DS) uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the VACS(D) components, for changes to the Department's mandated security controls.

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

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly 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 defining who can access the system, and at what privilege level are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed 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.)

11. Technologies

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

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes; continuous monitoring; checking the national vulnerability database (NVD); and following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any Information Technology. VACS(D) has been designed to minimize risk to privacy data. Please refer to 11(b) for further information.

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

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.